AUTOMATIONWORX

User Manual

UM EN FL SWITCH LM

Order No.: 2888851

Hardware and Software of Lean Managed Switches

PHOENIX CONTACT
INSPIRING INNOVATIONS

AUTOMATIONWORX

User Manual

Hardware and Software of Lean Managed Switches

05/2007

Designation: UM EN FL SWITCH LM

Revision: 01

Order No.: 2888851

This user manual is valid for:

Designation	Order No.
FL SWITCH LM 8TX	2832632
FL SWITCH LM 4TX/2FX	2832658
FL SWITCH LM 4TX/2FX SM	2891916
FL SWITCH LM 8TX-E	2891466
FL SWITCH LM 4TX/2FX-E	2891660
FL SWITCH LM 4TX/2FX SM-E	2891864

Please Observe the Following Notes

In order to ensure the safe use of the product described, we recommend that you read this manual carefully. The following notes provide information on how to use this manual.

User Group of This Manual

The use of products described in this manual is oriented exclusively to qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.

Phoenix Contact accepts no liability for erroneous handling or damage to products from Phoenix Contact or third-party products resulting from disregard of information contained in this manual.

Explanation of Symbols Used

The *attention* symbol refers to an operating procedure which, if not carefully followed, could result in damage to hardware and software or personal injury.

The *note* symbol informs you of conditions that must be strictly observed to achieve error-free operation. It also gives you tips and advice on the efficient use of hardware and on software optimization to save you extra work.

The *text* symbol refers to detailed sources of information (manuals, data sheets, literature, etc.) on the subject matter, product, etc. This text also provides helpful information for the orientation in the manual.

We Are Interested in Your Opinion

We are constantly striving to improve the quality of our manuals.

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send us your comments.

PHOENIX CONTACT GmbH & Co. KG
Documentation Services
32823 Blomberg
Germany

Phone +49 - 52 35 - 30 0
Fax + 49 - 52 35 - 34 20 21
E-mail tecdoc@phoenixcontact.com

General Terms and Conditions of Use for Technical Documentation

Phoenix Contact GmbH & Co. KG reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular data sheets, installation instructions, manuals, etc.) does not constitute any further duty on the part of
Phoenix Contact GmbH & Co. KG to furnish information on alterations to products and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact GmbH & Co. KG.
Please note that the supplied documentation is product-specific documentation only and that you are responsible for checking the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations.
Although Phoenix Contact GmbH & Co. KG makes every effort to ensure that the information content is accurate, up-to-date, and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact GmbH & Co. KG does not offer any guarantees as to the reliability, accuracy or completeness of the information.
All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

Phoenix Contact GmbH & Co. KG accepts no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, installation instructions, manuals, etc.).

The aforementioned limitations of liability and exemptions from liability do not apply, in so far as liability must be assumed, e.g., according to product liability law, in cases of premeditation, gross negligence, on account of loss of life, physical injury or damage to health or on account of the violation of important contractual obligations. Claims for damages for the violation of important contractual obligations are, however, limited to contract-typical, predictable damages, provided there is no premeditation or gross negligence, or that liability is assumed on account of loss of life, physical injury or damage to health. This ruling does not imply a change in the burden of proof to the detriment of the user.

Statement of Legal Authority

This manual, including all illustrations contained herein, is copyright protected. Use of this manual by any third party is forbidden. Reproduction, translation, and public disclosure, as well as electronic and photographic archiving or alteration requires the express written consent of Phoenix Contact. Violators are liable for damages.

Phoenix Contact reserves all rights in the case of patent award or listing of a registered design.Third-party products are always named without reference to patent rights. The existence of such rights shall not be excluded.

Internet

Up-to-date information on Phoenix Contact products can be found on the Internet at:

www.phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:

www.download.phoenixcontact.com

A conversion table is available on the Internet at:

www.download.phoenixcontact.com/general/7000_en_00.pdf

The switch is designed for SELV operation according to IEC 950 / EN 60950 / VDE 0805. Only SELV according to defined standards may be used to supply and connect the alarm contact.

The shielding ground of the connected twisted-pair cables is electrically connected with the front plate. When connecting network segments, avoid ground loops, potential transfers, and voltage equalization currents using the braided shield.

Electrostatic Discharge!

The module contains components that can be damaged or destroyed by electrostatic discharge. When handling the module, observe the necessary safety precautions against electrostatic discharge (ESD), in accordance with EN 61340-5-1 and EN 61340-5-2, as well as IEC 61340-5-1 and IEC 61340-5-2.

Only authorized Phoenix Contact personnel are permitted to open the housing.

Table of Contents

1 Lean Managed Switch 1-1

1.1 Properties 1-1
1.1.1 Front View/Operating Elements/Slots for the LMS 1-2
1.1.2 Dimensions of the LMS 1-3
1.1.3 Status and Diagnostic Indicators 1-3
1.2 Assembly/Removal 1-4
1.2.1 Assembly and Removal of the LMS 1-4
1.2.2 Assembly 1-4
1.2.3 Removal 1-5
1.3 Installing the Lean Managed Switch 1-5
1.3.1 Connecting the Supply Voltage 1-5
1.3.2 Alarm Contact 1-6
1.3.3 V.24 (RS-232) Interface for External Management 1-7
1.3.4 Grounding 1-7

2 Startup and Functions 2-1

2.1 Basic Settings 2-1
2.1.1 Default Upon Delivery/Default Settings 2-1
2.1.2 Assigning IP Parameters 2-1
2.1.3 Flowchart After a Restart 2-6
2.2 Frame Switching 2-8
2.2.1 Store-and-Forward 2-8
2.2.2 Multi-Address Function 2-8
2.2.3 Learning Addresses 2-8
2.2.4 Prioritization 2-9

3 Configuration and Diagnostics 3-1

3.1 Factory Manager 3-1
3.1.1 General Function 3-1
3.1.2 Assigning IP Parameters 3-1
3.1.3 Configuration and Diagnostics 3-3
3.2 Web-Based Management (WBM) 3-7
3.2.1 General Function 3-7
3.2.2 Requirements for the Use of WBM 3-8
3.2.3 Functions/Information in WBM 3-9
3.3 Simple Network Management Protocol (SNMP) 3-23
3.3.1 General Function 3-23
3.3.2 Diagram of SNMP Management 3-25
3.3.3 RFC1213-MIB - MIB II 3-27
3.3.4 Bridge MIB (1.3.6.1.2.1.17) 3-29
3.3.5 Private MIBs 3-32

3.4 Management via Local V.24 (RS-232) Communication Interface 3-51
3.4.1 General Function 3-51
3.4.2 User Interface Functions 3-52
3.4.3 Starting With Faulty Software 3-55

4 Rapid Spanning Tree 4-1

4.1 General Function 4-1
4.1.1 General Function 4-1
4.2 RSTP Startup 4-2
4.2.1 Enabling RSTP on All Switches Involved 4-2
4.2.2 Configuration Notes for Rapid Spanning Tree 4-16

5 Multicast Filtering 5-1

5.1 Basics 5-1
5.2 Dynamic Multicast Groups 5-1
5.2.1 Internet Group Management Protocol - IGMP 5-1
5.2.2 "General Multicast Configuration" Website 5-2

6 Technical Data 6-1

6 Ordering Data 6-2

1 Lean Managed Switch

1.1 Properties

The **L**ean **M**anaged **S**witch (**LMS**) is an Ethernet switch, which is suitable for industrial use. The LMS has eight or six ports, but with three versions available:

– FL SWITCH LM 8TX(-E) with eight RJ45 ports
– FL SWITCH LM 4TX/2FX(-E) with four RJ45 ports and two FX ports (multi-mode)
– FL SWITCH LM 4TX/2FX SM(-E) with four RJ45 ports and two FX ports (single mode)

Figure 1-1 Versions of the Lean Managed Switch

Future-Proof Networks for the Highest Possible Requirements

Maximum availability

Maximum Network Availability
A device design that does not use a fan, the redundant power supply, and conformance with all relevant industrial standards in terms of EMC, climate, mechanical load, etc. ensure the highest possible level of availability.
Redundancy can also be created with standards: the Rapid Spanning Tree Protocol ensures the safe operation of the entire network regardless of topology, even in the event of a cable interrupt.

All information

Clear Information
Two LEDs per port ensure that you always have sufficient local information. A web server and an SNMP agent are provided for diagnostics, maintenance, and configuration via the network. A terminal access point can be used for local operation.

Features and Fields of Application of the LMS

– Increased network performance by filtering data traffic:
  - Local data traffic remains local.
  - The data volume in the network segments is reduced.
– Easy network expansion and network configuration.
– Coupling segments with different transmission speeds.
  Automatic detection of 10 Mbps or 100 Mbps data transmission rate for RJ45 ports.
– Increased availability through the use of redundant transmission paths in various topologies and meshed structures as a result of RSTP.
– The switches can be configured using web-based management, SNMP or locally via a V.24 (RS-232) interface.

1.1.1 Front View/Operating Elements/Slots for the LMS

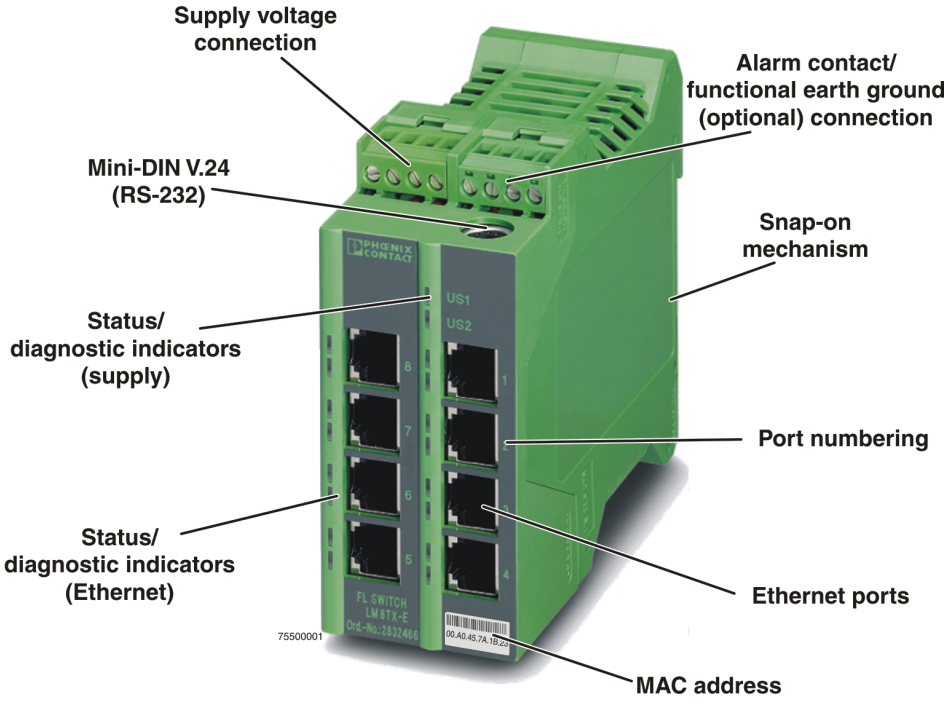


Figure 1-2 Front view/operating elements/slots for the LMS

– Diagnostic/status indicators
  Important information is displayed directly on the device. Each port has two LEDs. The top LED always indicates "LNK/ACT", the bottom LED indicates the data transmission rate.
– Diagnostic and status LEDs
  Two status and diagnostic LEDs are available for the supply voltage and for each port.
– Mini-DIN V.24 (RS-232)
  V.24 (RS-232) interface in Mini-DIN format for local configuration via the serial interface.

– Alarm contact/functional earth ground
  The floating alarm contact and the optional functional earth ground can be connected here via the COMBICON connector.
– Supply voltage connection
  The supply voltage can be connected redundantly via the 4-pos. COMBICON connector as an option.

1.1.2 Dimensions of the LMS

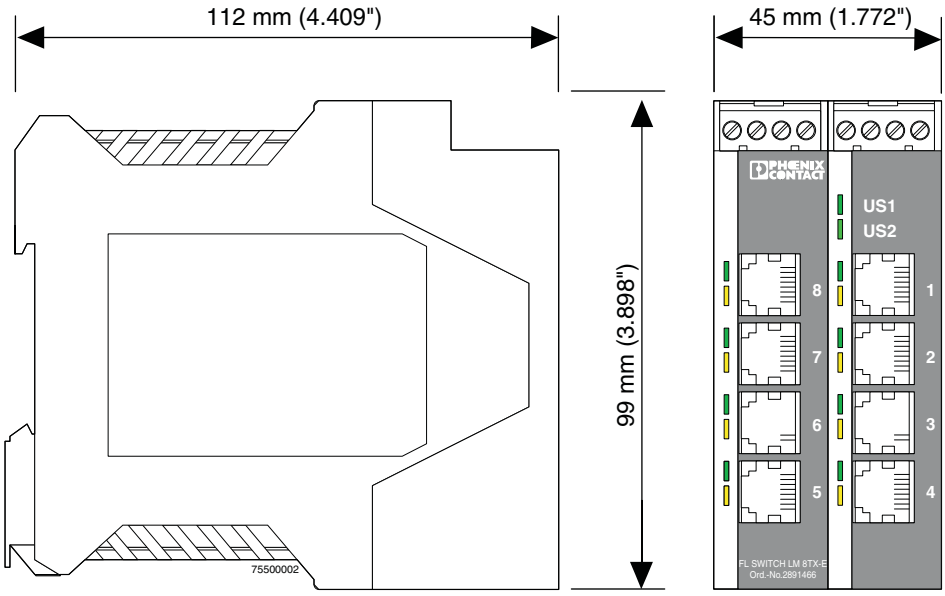


Figure 1-3 Housing dimensions of the LMS in millimeters (inches)

1.1.3 Status and Diagnostic Indicators

Des.	Color	Status	Meaning
US1	Green	ON	Supply voltage US1 in the tolerance range
		OFF	Supply voltage US1 less than 18 V DC
US2	Green	ON	Supply voltage US2 in the tolerance range
		OFF	Supply voltage US2 less than 18 V DC
LNK	Green	ON	Link active
		OFF	Link not active
		Flashing	Transmitting/receiving
100	Yellow	ON	Full duplex mode
		OFF	Half duplex mode
		Flashing	Collision detected

1.1.4 Firmware Versions and Their Functions

For the following switch versions (LM)

FL SWITCH LM 8TX

FL SWITCH LM 4TX/2FX

FL SWITCH LM 4TX/2FX SM

Firmware Version 1.04 provides the standard switch functions.

Firmware 2.02 offers the following additional functions:

– Multicast filter mechanisms
– IGMP snooping and querier function
– Port mirroring
– Port statistic
– Link status via alarm contact
– MAC address clearing

For the following switch versions (LM-E)

– FL SWITCH LM 8TX-E
– FL SWITCH LM 4TX/2FX-E
– FL SWITCH LM 4TX/2FX SM-E

Firmware 1.11 offers the following functions:

– Multicast filter mechanisms
– IGMP snooping and querier function
– MAC address clearing

1.2 Assembly/Removal

1.2.1 Assembly and Removal of the LMS

Mount the LMS on a clean DIN rail according to DIN EN 50 022 (e.g., NS 35 ... from Phoenix Contact). To avoid contact resistance only use clean, corrosion-free DIN rails. Before mounting the modules, an end clamp (E/NS 35N, Order No. 0800886) should be mounted on the left-hand side next to the LMS to stop the modules from slipping on the DIN rail. The end clamp should only be mounted on the right-hand side once the LMS has been mounted.

1.2.2 Assembly

1. Place the module onto the DIN rail from above (A). The upper holding keyway must be hooked onto the top edge of the DIN rail. Push the module from the front towards the mounting surface (B).

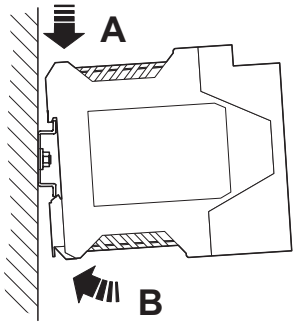


Figure 1-4 Snapping the LMS onto the DIN rail

2. Once the module has been snapped on properly, check that it is fixed securely on the DIN rail. Check whether the positive latches are facing upwards, i.e., snapped on correctly.

1.2.3 Removal

1. Remove all connectors.
2. Pull down the positive latches using a suitable tool (e.g., screwdriver). Both positive latches remain snapped out. Then swivel the bottom of the module away from the DIN rail slightly (A). Next, lift the module upwards away from the DIN rail (B).

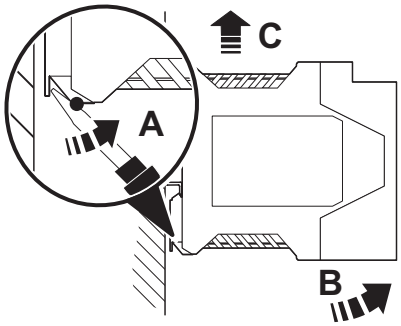


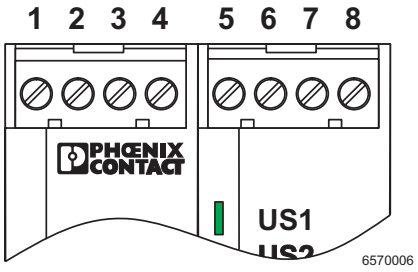
Figure 1-5 Removal of the LMS

1.3 Installing the Lean Managed Switch

1.3.1 Connecting the Supply Voltage

1.3.1.1 Assignment of the COMBICON Connector

Terminal	Meaning
1	Supply voltage +US1
2	GND US1
3	Supply voltage +US2
4	GND US2
5 and 6	Floating alarm contact
7	Functional earth ground (optional)
8	Not used



24 V DC

The LMS is operated with a 24 V DC voltage that can be supplied redundantly, if required (see Figure 1-6 version 2)

If redundant power supply monitoring is active (default setting), an error is indicated if only one voltage is applied. A bridge between US1 and US2 prevents this error message. It is also possible to deactivate monitoring in web-based management.

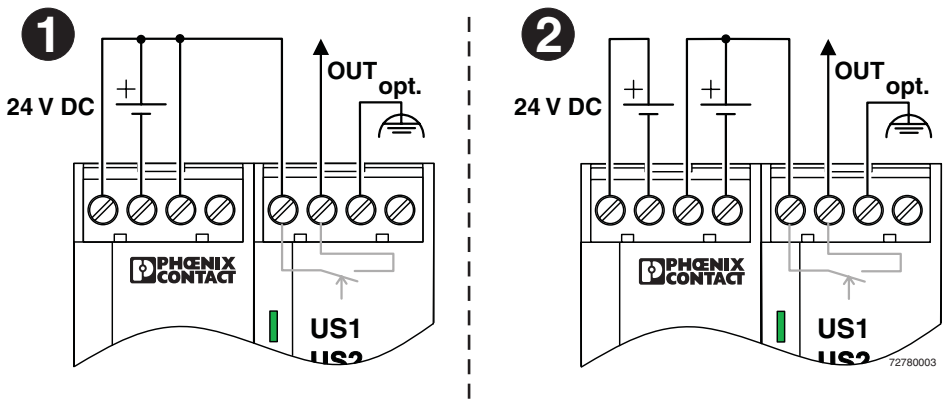


Figure 1-6 LMS supply

1.3.2 Alarm Contact

The switch has a floating alarm contact. Under normal conditions, the contact is closed allowing current to flow. When power is lost, the contact opens, indicating an error.

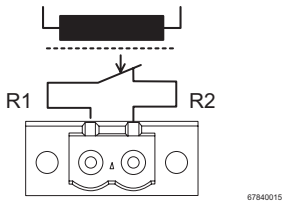


Figure 1-7 Circuit diagram for the alarm contact

In the event of non-redundant power supply, the switch indicates a supply voltage failure by opening the alarm contact. This error message can be prevented by connecting the supply voltage to both terminals in parallel, as shown in Figure 1-6, or by deactivating redundant power supply monitoring in web-based management.

1.3.3 V.24 (RS-232) Interface for External Management

The 6-pos. Mini-DIN female connector provides a serial interface to connect a local management station. Use the "PRG CAB MINI DIN" programming cable (Order No. 2760611). It can be used to connect a VT100 terminal or a PC with corresponding terminal emulation to the management interface (for an appropriate cable, please refer to "Ordering Data" on page 6-2). Set the following transmission parameters:

Bits per second	38400
Data bits	8
Parity	None
Stop bits	1
Flow control	None

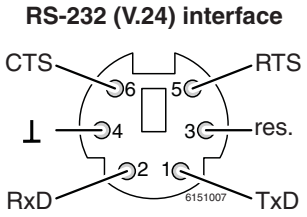


Figure 1-8 Transmission parameters and assignment of the V.24 (RS-232) interface

1.3.4 Grounding

Grounding protects people and machines against hazardous voltages. To avoid these dangers, correct installation, taking the local conditions into account, is vital.

All Factory Line devices must be grounded so that any possible interference is shielded from the data telegram and discharged to ground potential.

A wire of at least 2.5 mm^2 must be used for grounding. When mounting on a DIN rail, the DIN rail must be connected with protective earth ground using grounding terminal blocks. The module is connected to protective earth ground via a metal clip on the rear of the housing.

Option: In an environment particularly prone to EMI, noise immunity can be increased by an additional low-impedance connection to functional earth ground via terminal 7 ("Assignment of the COMBICON Connector" on page 1-6).

2 Startup and Functions

By default upon delivery the IGMP Snooping function is activated for the „E“ versions. It can be activated in the WBM for the other versions, if necessary.

2.1 Basic Settings

The basic Ethernet functions do not have to be configured and are available when the supply voltage is switched on.

2.1.1 Default Upon Delivery/Default Settings

By default upon delivery or after the system is reset to the default settings, the following functions and properties are available:

– The password is "private".
– All IP parameters are deleted. The switch has **no** valid IP parameters:
  IP address: 0.0.0.0
  Subnet mask: 0.0.0.0
  Gateway: 0.0.0.0
– BootP is activated as the addressing mechanism.
– All available ports are activated with the following parameters:
  - Auto negotiation and auto crossing for RJ45 ports.
  - 100 Mbps - full duplex for FX ports.
– All information collected by the SNMP agent is deleted.
– The web server, SNMP agent, and V.24 (RS-232) interface are active.
– The "Rapid Spanning Tree" WBM configuration page is activated.
– The alarm contact only opens in the event of non-redundant power supply.
– The aging time is set to 48 seconds.

2.1.2 Assigning IP Parameters

When the supply voltage is switched on, the switch sends requests (BootP requests) to assign IP parameters.

The "BootP" function can be deactivated via the management. By default upon delivery, the "BootP" function is activated.

The assignment of valid IP parameters is vital to the management function of the switch.

Options for Assigning IP Parameters:

– Configuration via the BootP protocol (default upon delivery)
– Static configuration via the management interfaces

The assignment of IP parameters with Factory Manager 2.1 is described on page 3-1.

2.1.2.1 Valid IP Parameters

IP parameters comprise the following three elements: "IP address", "subnet mask", and "default gateway/router".

Valid IP addresses are:
000.000.000.001 to 126.255.255.255
128.000.000.000 to 223.255.255.255

Valid multicast addresses are:
224.000.000.001 to 239.255.255.255

Valid subnet masks are:
255.000.000.000 to 255.255.255.252

Default gateway/router:
The IP address of the gateway/router must be in the same subnetwork as the address of the switch.

2.1.2.2 Assigning IP Addresses

The IP address is a 32-bit address, which consists of a network part and a user part. The network part consists of the network class and the network address.
There are currently five defined network classes; Classes A, B, and C are used in modern applications, while Classes D and E are hardly ever used. It is therefore usually sufficient if a network device only "recognizes" Classes A, B, and C.

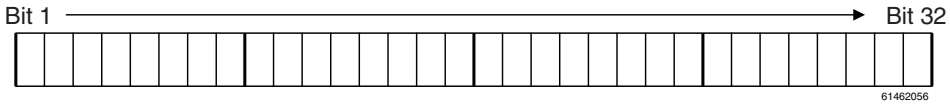


Figure 2-1 Position of bits within the IP address

With binary representation of the IP address the network class is represented by the first bits. The key factor is the number of "ones" before the first "zero". The assignment of classes is shown in the following table. The empty cells in the table are not relevant to the network class and are already used for the network address.

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5
Class A	0				
Class B	1	0			
Class C	1	1	0		
Class D	1	1	1	0	
Class E	1	1	1	1	0

The bits for the network class are followed by those for the network address and the user address. Depending on the network class, a different number of bits are available, both for the network address (network ID) and the user address (host ID).

	Network ID	Host ID
Class A	7 bits	24 bits
Class B	14 bits	16 bits
Class C	21 bits	8 bits
Class D	28-bit multicast identifier	
Class E	27 bits (reserved)	

IP addresses can be represented in decimal or hexadecimal form. In decimal notation, bytes are separated by dots (dotted decimal notation) to show the logical grouping of the individual bytes.

The decimal points do not divide the address into a network and user address. Only the value of the first bits (before the first "zero") specifies the network class and the number of remaining bits in the address.

Possible Address Combinations

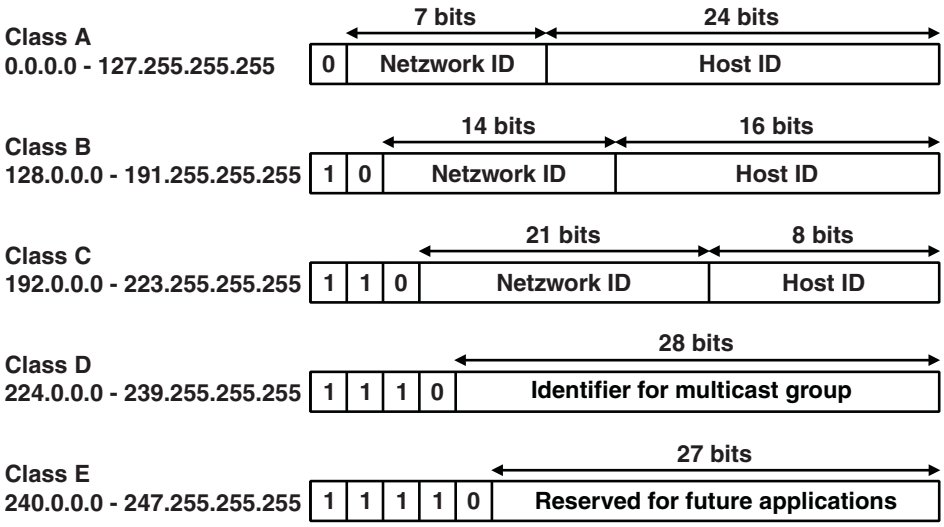


Figure 2-2 Structure of IP addresses

2.1.2.3 Special IP Addresses for Special Applications

Certain IP addresses are reserved for special functions. The following addresses should not be used as standard IP addresses.

127.x.x.x Addresses

The Class A network address "127" is reserved for a loopback function on all computers, regardless of the network class. This loopback function may only be used on networked computers for internal test purposes.

If a telegram is addressed to a computer with the value 127 in the first byte, the receiver immediately sends the telegram back to the transmitter.

The correct installation and configuration of the TCP/IP software, for example, can be checked in this way.

As Layers 1 and 2 of the ISO/OSI reference model are not included in the test they should be tested separately using the ping function.

Value 255 in the Byte

Value 255 is defined as a broadcast address. The telegram is sent to all the computers that are in the same part of the network. Examples: 004.255.255.255, 198.2.7.255 or 255.255.255.255 (all the computers in all the networks). If the network is divided into subnetworks, the subnet masks must be observed during calculation, otherwise some devices may be omitted. Simplified: The last address of an area is reserved as the broadcast address.

0.x.x.x Addresses

Value 0 is the ID of the specific network. If the IP address starts with a zero, the receiver is in the same network. Example: 0.2.1.1 refers to device 2.1.1 in this network.

The zero previously signified the broadcast address. If older devices are used, unauthorized broadcast and complete overload of the entire network (broadcast storm) may occur when using the IP address 0.x.x.x.

2.1.2.4 Subnet Masks

Routers and gateways divide large networks into several subnetworks. The IP addresses for individual devices are assigned to specific subnetworks by the subnet mask. The **network part** of an IP address is **not** modified by the subnet mask. An extended IP address is generated from the user address and subnet mask. Because the masked subnetwork is only recognized by the local computers, this extended IP address appears as a standard IP address to all the other devices.

Structure of the Subnet Mask

The subnet mask always contains the same number of bits as an IP address. The subnet mask has the same number of bits (in the same position) set to "one", which is reflected in the IP address for the network class.

Example: An IP address from Class A contains a 1-byte network address and a 3-byte computer address. Therefore, the first byte of the subnet mask may only contain "ones".

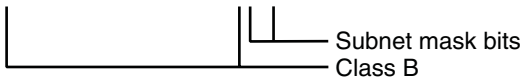
The remaining bits (three bytes) then contain the address of the subnetwork and the computer. The extended IP address is created when the bits of the IP address and the bits of the subnet mask are ANDed. Because the subnetwork is only recognized by local devices, the corresponding IP address appears as a "normal" IP address to all the other devices.

Application

If the ANDing of the address bits gives the local network address and the local subnetwork address, the device is located in the local network. If the ANDing gives a different result, the data telegram is sent to the subnetwork router.

Example for a Class B subnet mask:

Decimal representation: 255.255.192.0
Binary representation: 1111 1111.1111 1111.1100 0000.0000 0000



Using this subnet mask, the TCP/IP protocol software differentiates between the devices that are connected to the local subnetwork and the devices that are located in other subnetworks.

Example: Device 1 wants to establish a connection with device 2 using the above subnet mask. Device 2 has IP address 59.EA.55.32.

IP address display for device 2:

Hexadecimal representation: 59.EA.55.32
Binary representation: 0101 1001.1110 1010.0101 0101.0011 0010

The individual subnet mask and the IP address for device 2 are then ANDed bit-by-bit by the software to determine whether device 2 is located in the local subnetwork.

ANDing the subnet mask and IP address for device 2:

Subnet mask:		1111 1111.1111 1111.1100 0000.0000 0000
	AND	
IP address:		0101 1001.1110 1010.0101 0101.0011 0010
Result:		0101 1001.1110 1010.0100 0000.0000 0000

Subnetwork

After ANDing, the software determines that the relevant subnetwork (01) does not correspond to the local subnetwork (11) and the data telegram is forwarded to a subnetwork router.

2.1.3 Flowchart After a Restart

2.1.3.1 Loading the Configuration Data

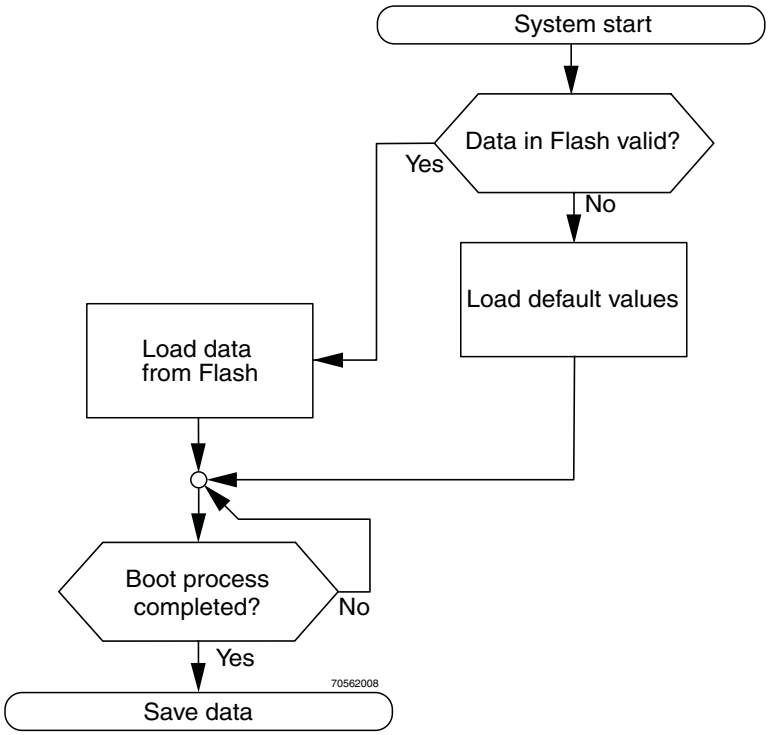


Figure 2-3 Flowchart: Loading the configuration data

2.1.3.2 Assigning IP Parameters

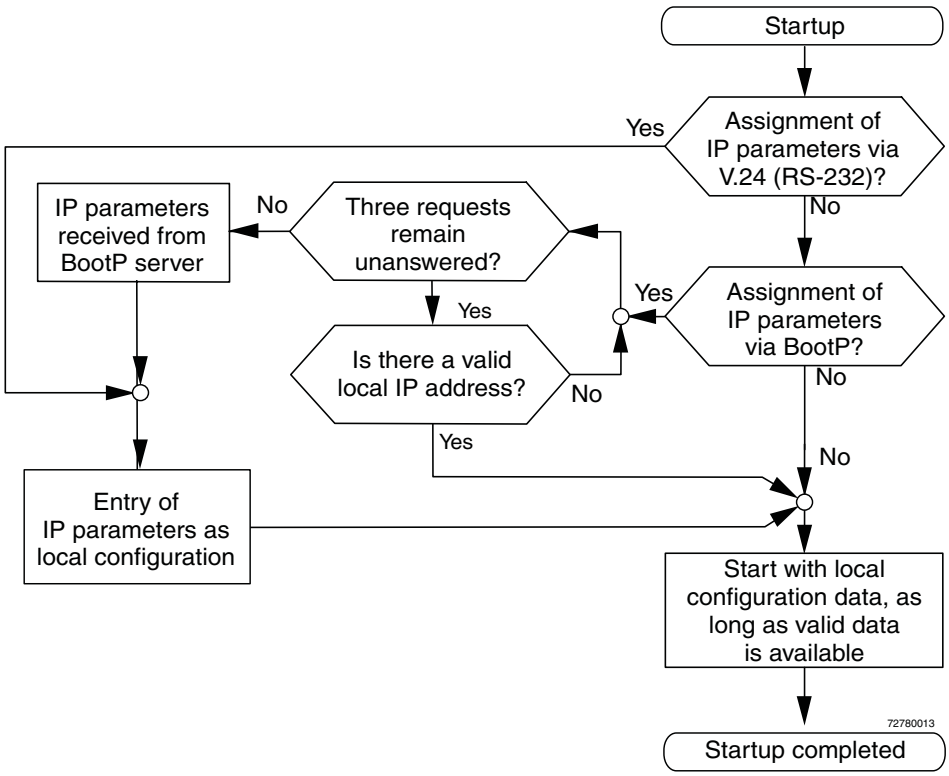


Figure 2-4 Flowchart: Assigning IP parameters

2.2 Frame Switching

The managed switch operates in store-and-forward mode. When receiving a data packet, the switch analyzes the source and destination addresses. The switch stores up to 1023 MAC addresses with an aging time of 48 seconds in its address table.

2.2.1 Store-and-Forward

All data telegrams that are received by the switch are saved and their validity is checked. Invalid or faulty data packets (> 1522 bytes or CRC errors) and fragments (< 64 bytes) are rejected. Valid data telegrams are forwarded by the switch.

2.2.2 Multi-Address Function

The switch learns all the source addresses for each port. Only packets with:

– Unknown source addresses
– A source address for this port
– A multicast/broadcast address

are forwarded to the destination address field via the relevant port. The switch can learn up to 1023 addresses. This is important when more than one termination device is connected to one or more ports. In this way, several independent subnetworks can be connected to one switch.

2.2.3 Learning Addresses

The LMS independently learns the addresses for termination devices, which are connected via a port, by evaluating the source addresses in the data telegram. When the LMS receives a data telegram, it only forwards this data telegram to the port that connects to the specified device (if the address could be learned beforehand).
The LMS can learn up to 1023 addresses and stores them in its table. The switch monitors the age of the learned addresses. The switch automatically deletes address entries from its address table that have exceeded a specific age (48 seconds, aging time).

All learned entries are deleted on a restart.

Flowchart for "Learning Addresses" Using the Example of Unicast Addresses

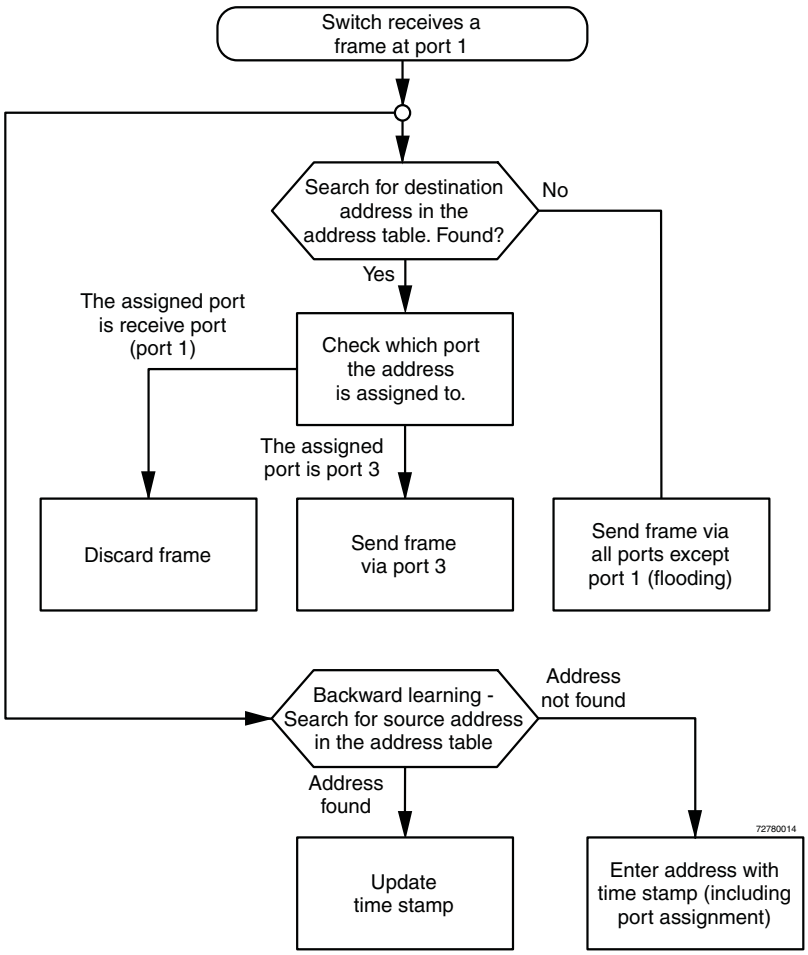

Switch receives a frame at port 1
Search for destination address in the address table. Found?
No
Yes
The assigned port is receive port (port 1)
Check which port the address is assigned to.
The assigned port is port 3
Discard frame
Send frame via port 3
Send frame via all ports except port 1 (flooding)
Backward learning - Search for source address in the address table
Address not found
Address found
72780014
Update time stamp
Enter address with time stamp (including port assignment)

Figure 2-5 Flowchart for "learning addresses"

2.2.4 Prioritization

The switch supports two priority queues for adjusting the internal packet processing sequence (traffic classes according to IEEE802.1D). Data telegrams that are received are assigned to these classes according to their priority, which is specified in the VLAN/prioritization tag:

– Data packets with values between "0" and "3" in the priority field are low (default) priority
– Data packets with values between "4" and "7" in the priority field are high priority and transmitted via the switch

2.2.4.1 VLAN/Prioritization Tag

The LMS processes incoming data packets with regard to prioritization information contained in the Ethernet packet (VLAN/prioritization tag).
The tag enables the specification of a priority level from 0 to 7, which the LMS assigns to one of its two internal queues. By default upon delivery, the packets with priorities from 0 to 3 are treated as low-priority packets whereas packets with priorities from 4 to 7 are high-priority Ethernet packets.

Processing Rules

The switch controller in the LMS forwards received packets to one of the receive queues according to the following decisions:

– BPDU packets are always assigned to the high-priority queue.
– Packets with unknown unicast addresses are always assigned to the low-priority queue.
– Packets are assigned to the high-priority queue if the priority from the VLAN/prioritization tag is mapped to the "high" level (default priority 4 to 7).
– The internal port priority "high" results in priority level 7 handling, i.e., the basic settings for data packet assignment to the high-priority queue are made.
– All residual data is assigned to the low-priority queue.

2.2.4.2 Strict Priority

The switch supports two priority queues for adjusting the internal packet processing sequence (traffic classes according to IEEE 802.1D). Data telegrams that are received are assigned to these classes according to their priority, which is specified in the VLAN/prioritization tag:

– Data packets with values between "0" and "3" in the priority field are low priority (default).
– Data packets with values between "4" and "7" in the priority field are high priority and transmitted via the switch.

The LMS uses "Strict Priority" for transmitting data telegrams. First, **all** high-priority data packets are assigned, once these are forwarded, low-priority telegrams are assigned.

This function prevents delays in high-priority data transmission, due to large volumes of low-priority data traffic. Low-priority traffic is rejected when the memory or data channel is overloaded.

3 Configuration and Diagnostics

Lean Managed Switches offer several user interfaces for accessing configuration and diagnostic data. The preferred interfaces are the web interface and SNMP interface. These two interfaces can be used to make all the necessary settings and request all information. Access via V.24 (RS-232) interface only enables access to basic information. However, the V.24 (RS-232) interface also enables firmware update via XMODEM in the event of faulty firmware.

Settings are not automatically saved permanently. The active configuration can be saved permanently by selecting "Save current configuration" on the "Configuration Management" web page, the "SAVE" button in the terminal interface or the "flWorkFWCtrlConfSave" SNMP object.

3.1 Factory Manager

3.1.1 General Function

The integration of the LMS in the Factory Manager provides support for configuration and management.

3.1.2 Assigning IP Parameters

Only **one** of several options for assigning IP parameters using the Factory Manager is described here.

The free-of-charge „IPAssign.exe“ addressing tool can be used to assign the IP parameters. It is not necessary to install the program as it is available in the form of an executable (*.exe) file. It can be downloaded at www.download.phoenixcontact.com.

Once you have established all the necessary connections and the Factory Manager has been started, restart the LMS.

Following the boot phase, the LMS sends the BootP requests, which are received by the Factory Manager and displayed in the message window. If you are operating other devices in the same network, messages from these devices may also be displayed. Messages from Phoenix Contact Factory Line components can be easily identified by their MAC address, which starts with 00.A0.45... and is provided on the devices.

Please check the MAC address in the messages to ensure the correct device is addressed.

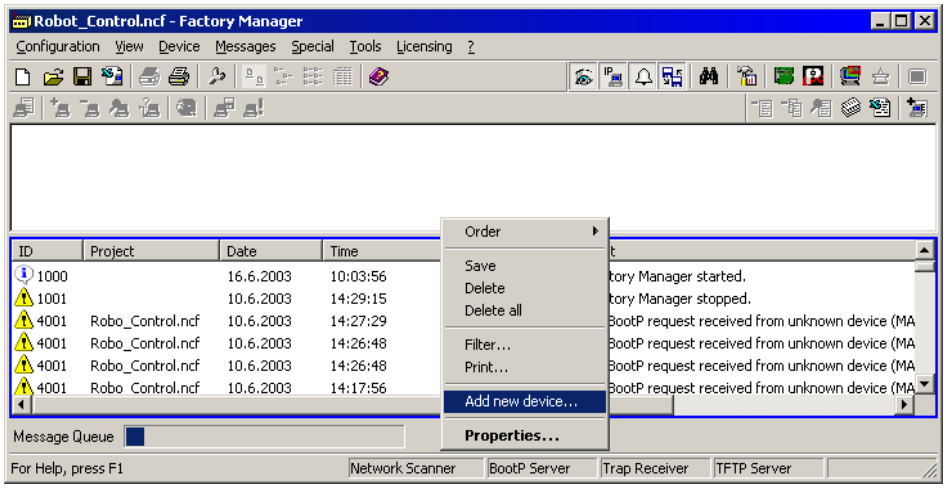


Figure 3-1 Messages from the LMS in the Factory Manager

Right-click on one of the LMS messages and select the "Add new device..." menu item. Under "Description", select an icon and enter a device name.

Specify the desired IP parameters under "TCP/IP" (see also "Assigning IP Parameters" on page 3-1).

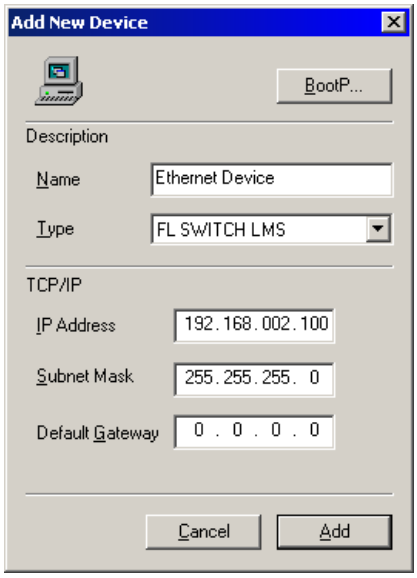


Figure 3-2 Input mask for IP parameters

Make sure that the assignment of IP parameters via BootP is also activated.

Once you have clicked on "Add", the device is added to the project and is indicated as **unavailable**. You must now restart or reset the LMS. Following a restart, the LMS resends the BootP requests and receives the corresponding BootP reply from the Factory Manager. Once the boot process has been completed the LMS is indicated as available.

If the LMS is still indicated as "unavailable", check your network card settings. Please note that both devices must be located in the same network/subnetwork. If the Factory Manager receives the BootP requests this does not mean that the devices are located in the same subnetwork, as the BootP requests are sent as a broadcast beyond subnetwork boundaries.

3.1.3 Configuration and Diagnostics

Numerous options for configuring and diagnosing the LMS can be found in the "Device" menu under "Properties".

General

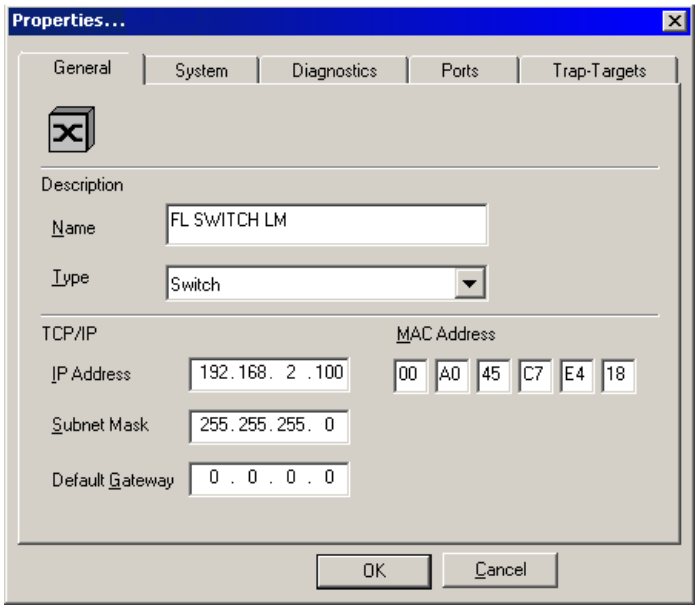


Figure 3-3 "General" menu

Here you can check or modify device names and types as well as IP parameters.

If you modify the IP address and/or the other IP parameters using the Factory Manager, once you click "OK" you will no longer have access via the Factory Manager. Restarting the LMS activates the modified parameters and restores access.

To activate the new addresses following a restart, BootP must be activated in the LMS.

System

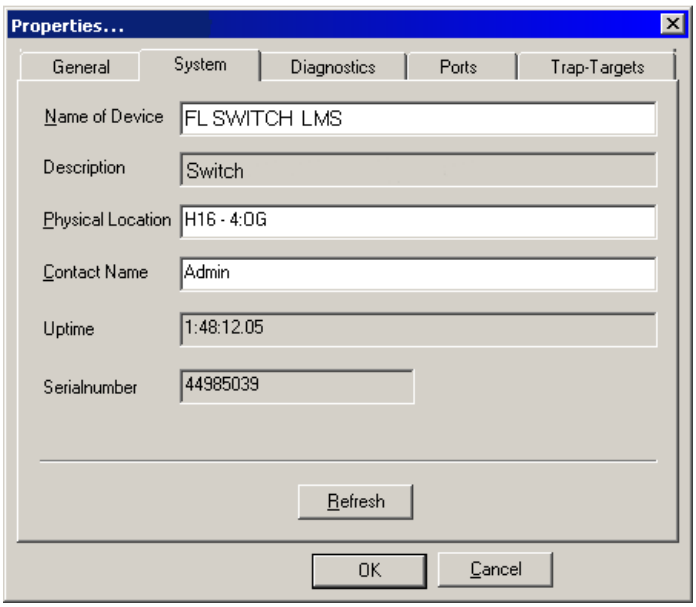


Figure 3-4 "System" menu

In this menu, you can add additional information in the white fields, which will be saved on the LMS. This information is also available via SNMP and WBM.

Diagnostics

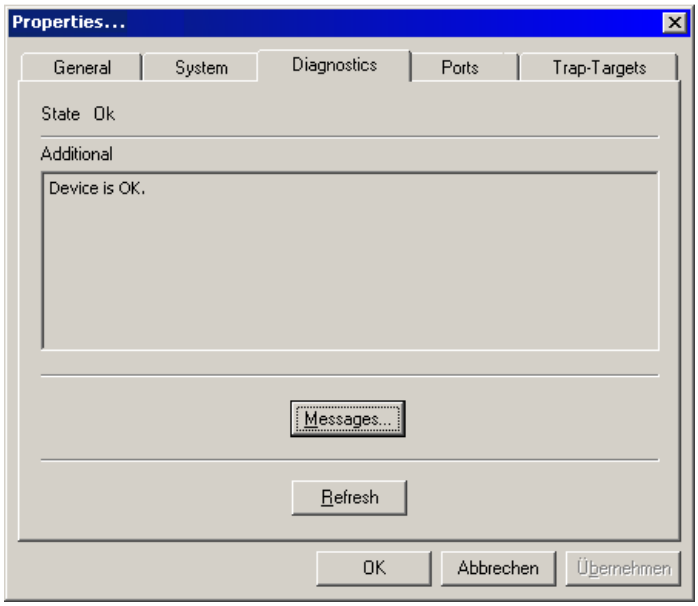


Figure 3-5 "Diagnostics" menu

Information about the device status and redundancy is displayed here. All the messages for this device are displayed under Messages.

Trap Targets

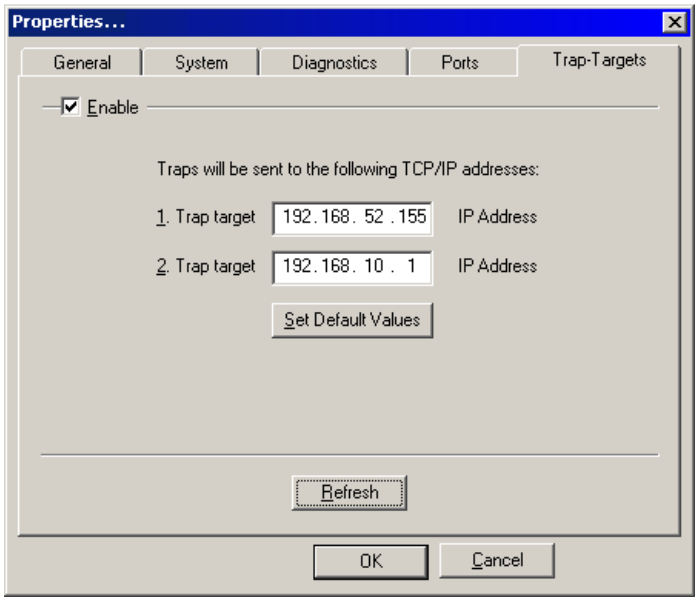


Figure 3-6 "Trap Targets" menu

Trap targets are displayed or set here, and the "send traps" function can be activated or deactivated. Clicking on "Set Default Values" automatically activates the IP address of the computer on which the Factory Manger is installed as the trap target.

Firmware

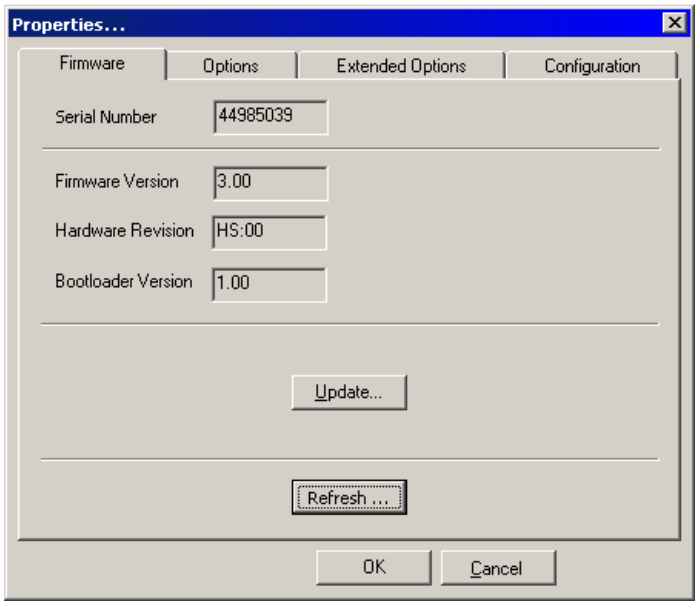


Figure 3-7 "Firmware" menu

Here you can view all information about the current device software (firmware). You can also update the software using the Factory Manager.

Firmware update

When you click on "Update", the following window appears, which contains information about the firmware used.

Please make sure that the "TFTP Server" service program is activated in the toolbar.

Following a firmware update, a reset is executed **automatically** to activate the new firmware.

Firmware update can take several minutes. You can monitor the download in the message window (25%, 50%, 75%, 100%). Always wait until all the LEDs light up after approximately two minutes and the device is available again after booting.

It is not ensured that all existing configuration data will be retained after a firmware update/downgrade. Therefore, please check the configuration settings or return the device to the settings default upon delivery.

A voltage failure during a firmware update results in the destruction of the firmware on the LMS. An update via XMODEM is required, see "Starting With Faulty Software" on page 3-56.

Update

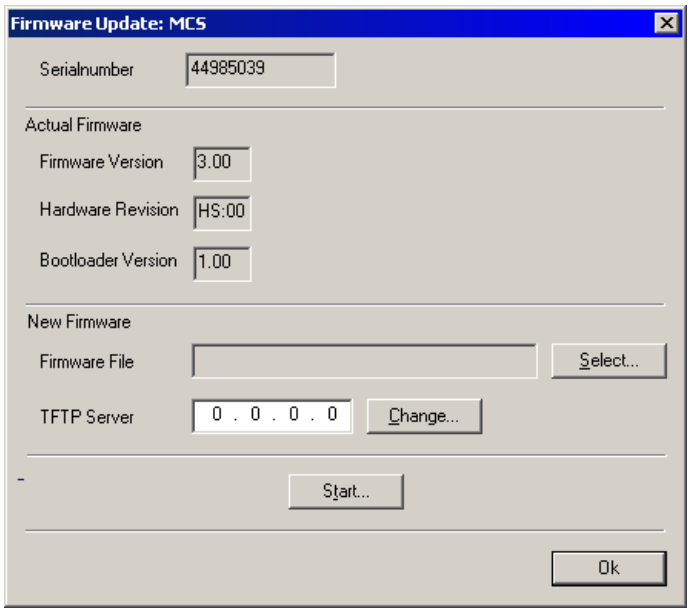


Figure 3-8 "Update" menu

In order to enable a firmware update, the firmware image must be located in the "Download" directory of the Factory Manager.

3.2 Web-Based Management (WBM)

3.2.1 General Function

Online diagnostics

The user-friendly web-based management interface can be used to manage the switch from anywhere in the network using a standard browser. Comprehensive configuration and diagnostic functions are clearly displayed on a graphic user interface. Every user with a network connection to the device has read access to that device via a browser. Depending on the physical structure of the switch, a wide range of information about the device itself, the set parameters, and the operating state can be viewed.

Modifications can only be made by entering the valid password. By default upon delivery, the password is "private".

For security reasons, we recommend you enter a new, unique password.

3.2.2 Requirements for the Use of WBM

As the web server operates using the Hyper Text Transfer Protocol, a standard browser can be used. Access is via the URL "http://IP address of the device".
Example: "http://172.16.29.112".
For full operation of the web pages, the browser must support JavaScript 1.2 and cascading style sheets Level 1. We recommend the use of Microsoft Internet Explorer 6.0.

WBM can only be called using a valid IP address. By default upon delivery, the switch has **no** valid IP address.

Settings are not automatically saved permanently. The active configuration can be saved permanently by selecting "Save current configuration" on the "Configuration Management" web page.

3.2.2.1 Structure of the Web Pages

The web pages are divided into four areas:

– Device type and device logo.
– Device name (assigned by the user) and loading time, to prevent mix-ups.
– Navigation tree on the left-hand side.
– Information tables, which contain current device information during runtime.

3.2.2.2 Password Concept

After having entered the valid password, no further entry of the password is necessary for a period of 300 s (default). After this period of time has elapsed or after clicking on "Logout", the password must be re-entered.

The period of time can be set using the "flWorkFWCtrlLoginExpire" SNMP object within a range of 30 s to 3600 s (default 300 s).

The concept is valid for the first ten users. All further users must confirm each modification of the configuration with the password.

3.2.3 Functions/Information in WBM

The navigation tree provides direct access to the following four areas:

– **General Instructions**
  Basic information about WBM.
– **Device Information**
  General device information.
– **General Configuration**
  General device configuration.
– **Switch Station**
  Device-specific configuration and diagnostics.

3.2.3.1 General Instructions

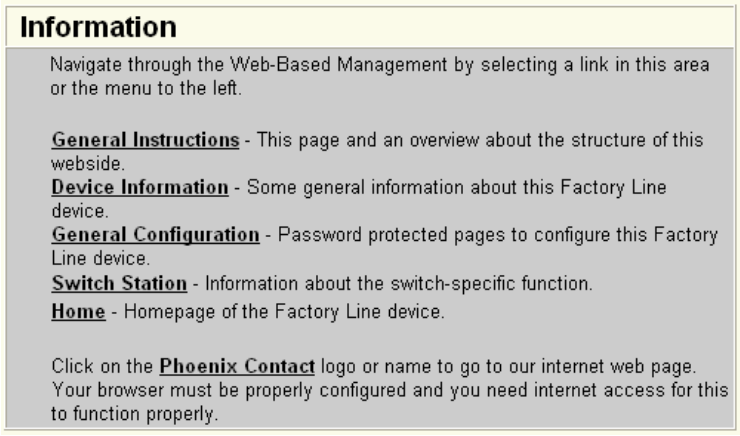

Information
Navigate through the Web-Based Management by selecting a link in this area or the menu to the left.
General Instructions - This page and an overview about the structure of this webside.
Device Information - Some general information about this Factory Line device.
General Configuration - Password protected pages to configure this Factory Line device.
Switch Station - Information about the switch-specific function.
Home - Homepage of the Factory Line device.
Click on the Phoenix Contact logo or name to go to our internet web page. Your browser must be properly configured and you need internet access for this to function properly.

Figure 3-9 "Information" web page

Contains a brief description of WBM and a navigation tree (site map), which is linked to every page of WBM.

3.2.3.2 Device Information

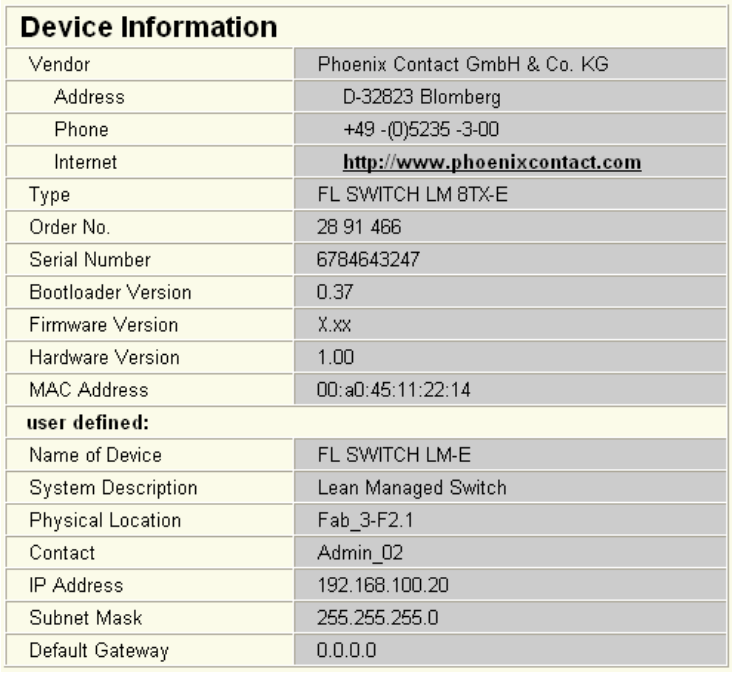


Figure 3-10 "Device Information" web page

"General" Menu

This page contains a range of static information about the device and the manufacturer.

"Local Diagnostics" Menu

This page describes the meaning of the diagnostic and status indicators.

Local Diagnostics	
Power Supply	
US1	Supply Voltage 1 (green LED)
US2	Supply Voltage 2 (green LED)
Green LED	
On	Link Up
Off	Link Down
Blink	Send or Receive Activity
Yellow LED	
On	Full Duplex Mode
Off	Half Duplex Mode
Blink	Collision Detection

Figure 3-11 "Local Diagnostics" web page

"Serial Port" Menu

This page lists the transmission parameters for serial communication.

Serial Port	
Baud Rate	38400
Character Size	8
Parity	None
Stop Bits	1
Flow Control	None

Figure 3-12 "Serial Port" menu

3.2.3.3 General Configuration

"IP Configuration" Menu

This page displays the set IP parameters and addressing mechanism. To change the IP parameters via WBM, "Static" assignment must be selected.

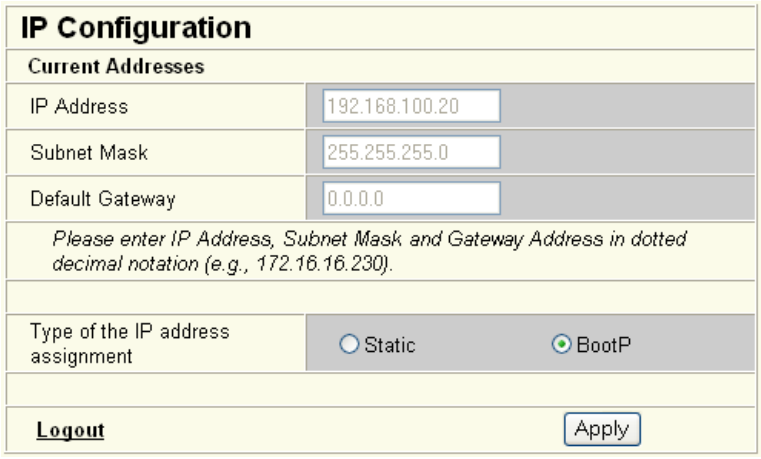


Figure 3-13 "IP Configuration" web page

If you modify the IP address and/or the other IP parameters via WBM, once you click on "Apply" you will no longer have access via the IP address set in the browser.

"SNMP Configuration" Menu

System information

This part of the table is used to display or modify user-specific device data, e.g., location, device name or function.

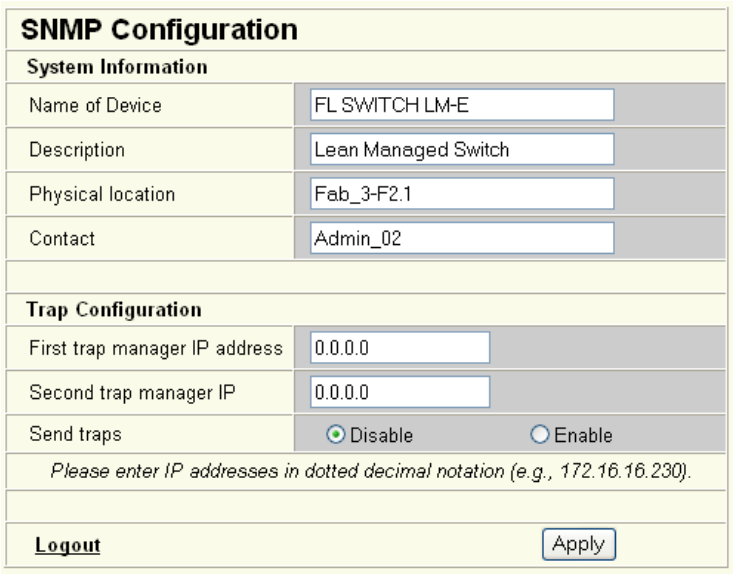


Figure 3-14 "SNMP Configuration" web page

Trap configuration

This part of the table is used to view or modify the IP addresses of the two trap receivers. It is also used to activate/deactivate the "send traps" function.

"Software Update" Menu

This page is used to view or modify the parameters for a software update and to trigger the update.

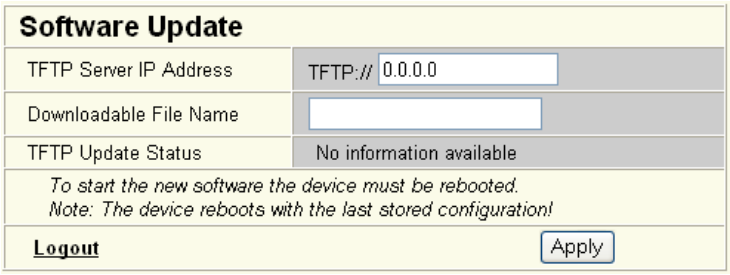


Figure 3-15 "Software Update" web page

3.2.4 Executing the Firmware/Software Update

Requirements

The device must have valid IP parameters so that the firmware can be updated. You also need a functional Factory Manager or another TFTP server.

A suitable version of the Factory Manager can be downloaded at www.download.phoenixcontact.com .

The following steps are required to update the software:

- Save the selected firmware/software in the download directory of your TFTP server. If you use the Factory Manager, the path for a standard installation is as follows: "C:\Programme\Phoenix Contact\Factory Manager\Version 2.3\download" or "C:\Program Files\Phoenix Contact\Factory Manager\Version 2.3\download".
- Start the Factory Manager and check whether the TFTP server is activated.

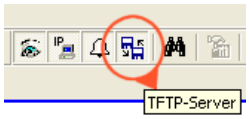


Figure 3-16 Factory Manager with TFTPserver activated

- Start the WBM of the switch and call the "Software Update" page (...General Configuration/Software Update).
- Enter the IP address of the computer on which the Factory Manager is installed in the "TFTP Server IP Address" field.
- Then enter the complete file name of the firmware file in "Downloadable File Name", but no path entries (no drive, no folder).

- Enter the device password (default: „private“) and click with the mouse on „Apply“.

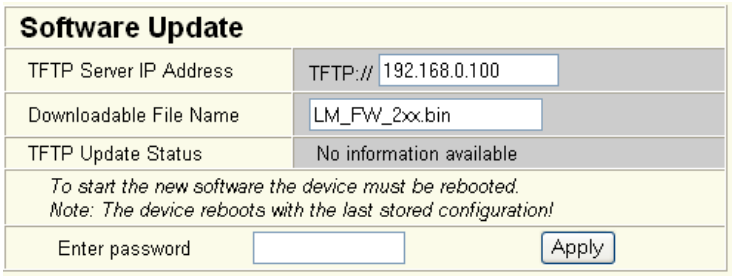


Figure 3-17 Web interface with the update parameters

Next this window.

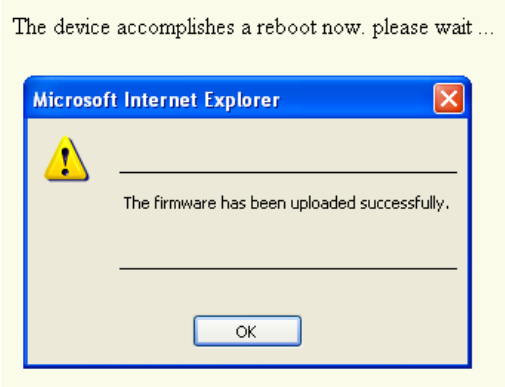

The device accomplishes a reboot now. please wait ...
Microsoft Internet Explorer
The firmware has been uploaded successfully.
OK

Figure 3-18 Message after a successful update

- Close the WBM and re-start it.

Please make sure that the "TFTP Server" service program is activated in the Factory Manager toolbar.

Firmware update can take several minutes. You can monitor the download in the Factory Manager message window (25%, 50%, 75%, 100%). Always wait until all the LEDs light up after approximately two minutes and the device is available again after booting.

It is not ensured that all existing configuration data will be retained after a firmware update/downgrade. Therefore, please check the configuration settings or return the device to the settings default upon delivery.

A voltage failure during a firmware update leads to the destruction of the LMS by the firmware. An update via XMODEM is required, see "Starting With Faulty Software" on page 3-56.

"Change Password" Menu

This option can be used to specify the current password and then enter a new, unique password. By default upon delivery, the password is "private" (please note that it is case-sensitive). For security reasons, the input fields do not display your password, but instead "*******" is displayed.

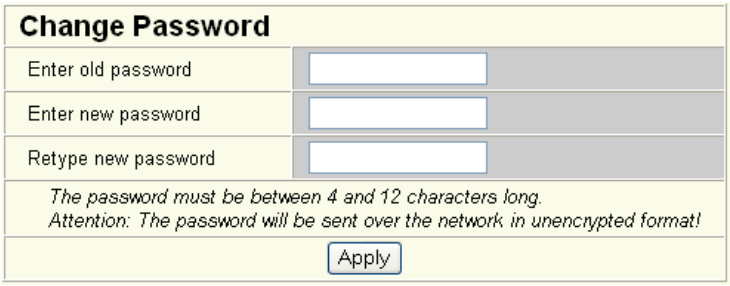

Change Password
Enter old password
Enter new password
Retype new password
The password must be between 4 and 12 characters long.
Attention: The password will be sent over the network in unencrypted format!
Apply

Figure 3-19 "Change Password" web page

The password must be between four and twelve characters long. Please note that the password is always transmitted via the network in unencrypted format.

Forgotten your password?
Call the Phoenix Contact phone number listed in the Appendix, making sure you have the device serial number and MAC address to hand.

"User Interfaces" Menu

The following actions can be executed here:

– Activation/deactivation of the web server.
– Activation/deactivation of the SNMP agent.
– Activation/deactivation of the configuration pages for redundancy.

With the activation/deactivation of the configuration pages under "User Interfaces", only the web pages for configuring the selected functions are enabled/disabled in the WBM menu.

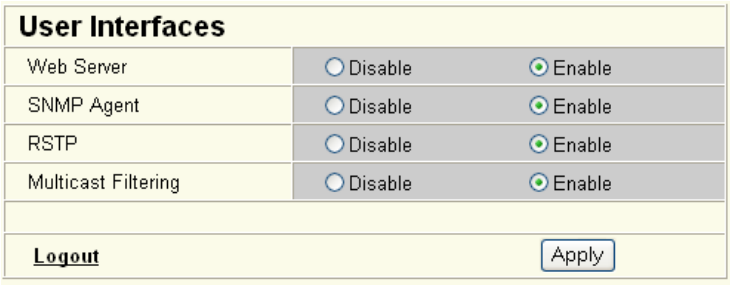


Figure 3-20 "User Interfaces" web page

"General Configuration/Configuration Management" Menu

This table is used to view all parameters that are required to save the active configuration or load a new configuration, and to modify them (by entering a valid password). It can also be used to restart the system with the relevant configuration.

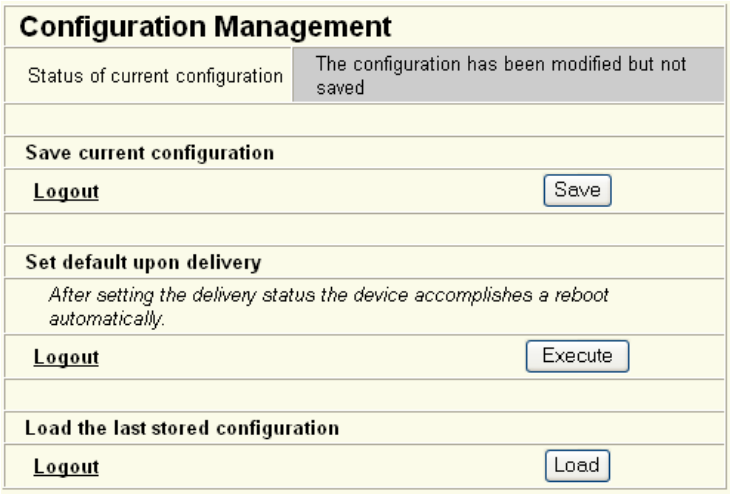


Figure 3-21 "Configuration Management" web page

Possible States for "Status of current configuration":

– The configuration has been modified but not saved.
– Saving the current configuration.
– The current configuration is equal to the one saved in the non-volatile memory of the switch.
– The current configuration was saved.

If the new configuration is not activated by a reset after a configuration download, the "Save current configuration" command overwrites the previously loaded configuration and instead saves the active configuration of the LMS.

Set default upon delivery

This option can be used to reset the switch to its default settings (default upon delivery) by entering a valid password.

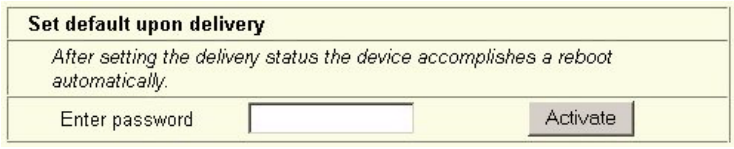

Set default upon delivery
After setting the delivery status the device accomplishes a reboot automatically.
Enter password
Activate

Figure 3-22 "Set default upon delivery" web page

WBM can only be called using a valid IP address. Once the switch has been reset to its default settings, it has **no** valid IP address.

Load the last stored configuration

This option can be used to reload the last configuration saved on the device or the PC. All modifications made to the configuration since it was last saved are lost.

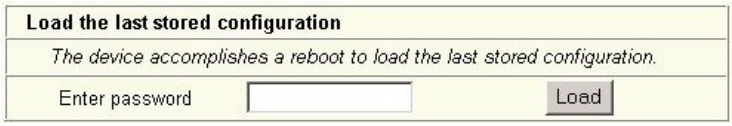

Load the last stored configuration
The device accomplishes a reboot to load the last stored configuration.
Enter password
Load

Figure 3-23 "Load the last stored configuration" web page

"General Configuration/Configuration Management/File Transfer" Menu

When a configuration is uploaded from the LMS to a PC, the last saved version is transmitted. If you want to transmit the active configuration, first save it again ("Save current configuration" function).

When a configuration is downloaded from the PC to an LMS, the new configuration is only activated once the switch has been reset.

The use of a configuration file does not affect an existing ("old") password.

Configuration using a configuration file is used when replacing devices. To duplicate devices using a configuration file, observe the following:

– Establish a point-to-point connection between an LMS and the management station.
– Load the configuration file to the LMS.
– Reset the LMS.
– Adjust the IP parameters.
– Save the configuration ("Save current configuration" function).

The duplicated switch can now be operated in the network using the adjusted IP parameters.

3.2.4.1 Switch Station

Reboot To trigger a reboot via the web interface, enter a valid password. Save the configuration beforehand, so that configuration modifications are retained or can be activated via a restart.

"Ports" Menu

Port Table Overview of all available ports. Clicking on the relevant port number opens a port-specific page ("Port Configuration").

Port Table

Port	Type	Port Status	Link State
1	TX 10/100	enable	100 Mbits FD
2	TX 10/100	enable	100 Mbits FD
3	TX 10/100	enable	100 Mbits FD
4	TX 10/100	enable	100 Mbits FD
5	TX 10/100	enable	not connected
6	TX 10/100	enable	100 Mbits FD
7	TX 10/100	enable	not connected
8	TX 10/100	enable	100 Mbits FD

Figure 3-24 "Port Table" web page

"Port Configuration Table" Menu (only FI Switch LM ...)

This menu provides an overview of the important configuration settings for all ports and also provides the option to set the status, transmission mode, and link monitoring function for all existing ports.

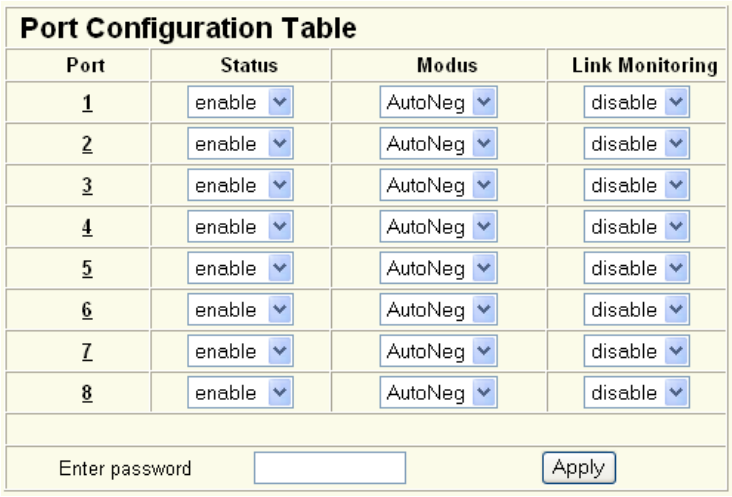


Figure 3-25 "Port Configuration Table" web page

Port Configuration Individual configuration option for each port. To view detailed data traffic statistics for the selected port, click on "Port Statistics".

Even if the port is switched off, the Link LEDs for the port remains active.

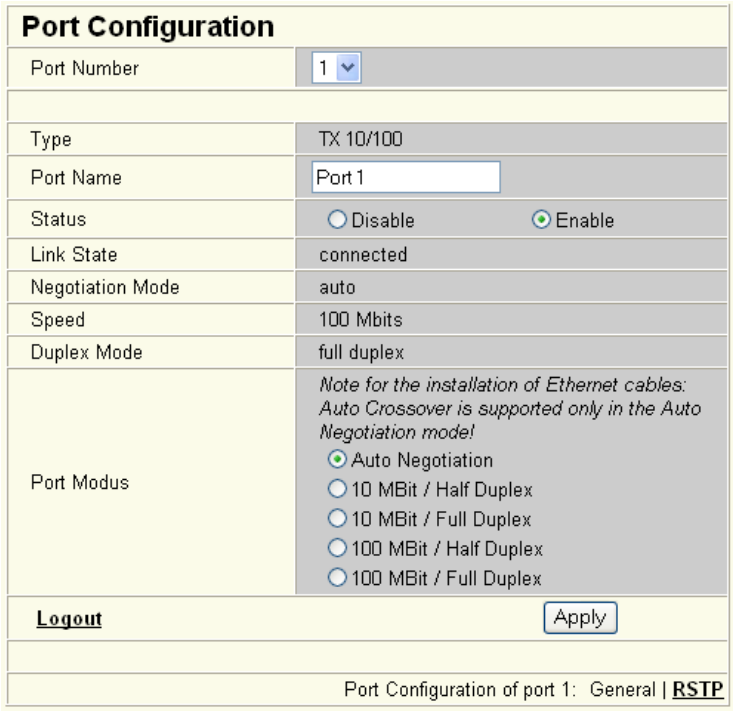

Port Configuration
Port Number 1
Type TX 10/100
Port Name Port 1
Status Disable Enable
Link State connected
Negotiation Mode auto
Speed 100 Mbits
Duplex Mode full duplex
Port Modus
Note for the installation of Ethernet cables: Auto Crossover is supported only in the Auto Negotiation mode!
Auto Negotiation
10 MBit / Half Duplex
10 MBit / Full Duplex
100 MBit / Half Duplex
100 MBit / Full Duplex
Logout
Apply
Port Configuration of port 1: General | RSTP

Figure 3-26 "Port Configuration" web page

"Ports/Port Statistics" Menu (only FL SWITCH LM ...)

This menu provides detailed statistical information about the volume of data for each individual port. On this page, additional counter states can be set to zero for all ports..

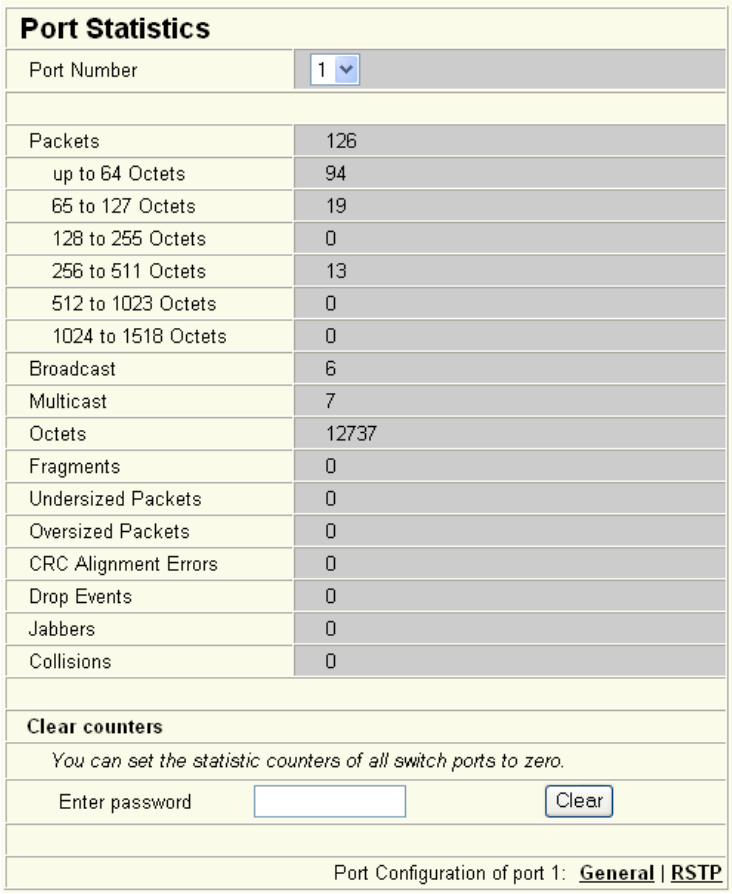


Figure 3-27 "Port Statistics" web page

"Ports/Port Mirroring" Menu

Activation/deactivation and setting of port mirroring. Port mirroring is used to passively read incoming or outgoing data that is being transmitted via the selected ports. To do this a measuring instrument (PC) is connected to the destination port, which records the data, yet must not itself be activated.

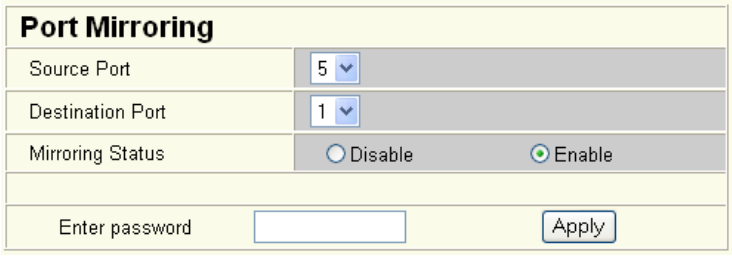


Figure 3-28 "Port Mirroring" web page

If ports are set with the same value, port mirroring will be disabled. The source port is set to "0".

The port capacity is calculated according to the set transmission parameters. Example: A source port is operated at 100 Mbps and reaches a capacity of 5%. The destination port is operated at 10 Mbps. Therefore, with the same volume of data the destination port reaches a capacity of 50%.

"Display" Menu

Here, you can find some status information about the swicth.

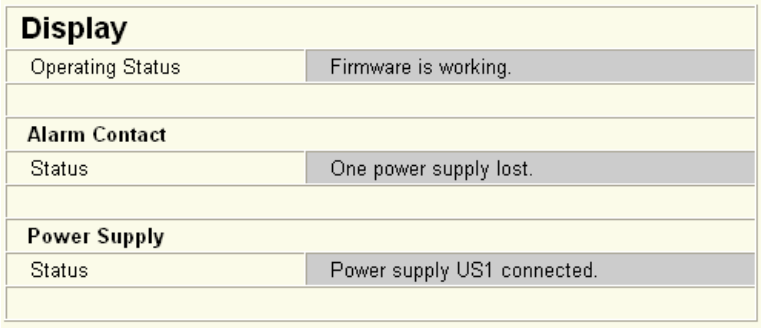


Figure 3-29 Menü „Display“

"Diagnostics/Alarm Contact" Menu

Here, you can set whether and for which events the alarm contact can be used.

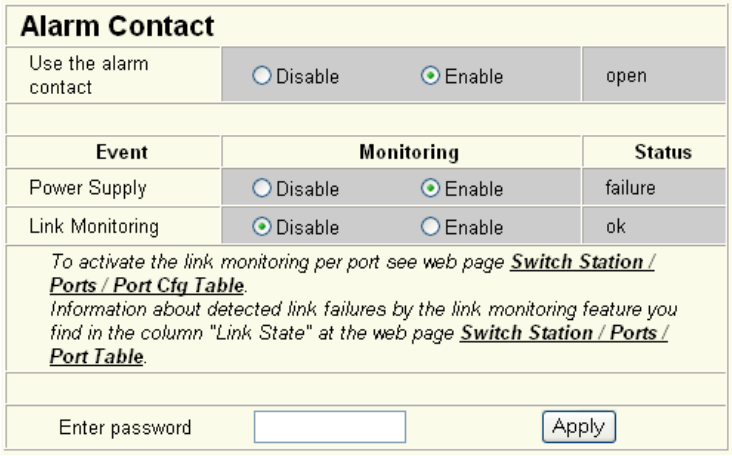


Figure 3-30 "Alarm Contact" web page

Click on the "Switch Station / Ports / Port Table" link (on "Alarm Contact" page in WBM) to access the port configuration page.

"Utilization" Menü

Here, the network capacity of every individual port is displayed as bargraph. The display is automatically updated in accordance with the refresh intervals.

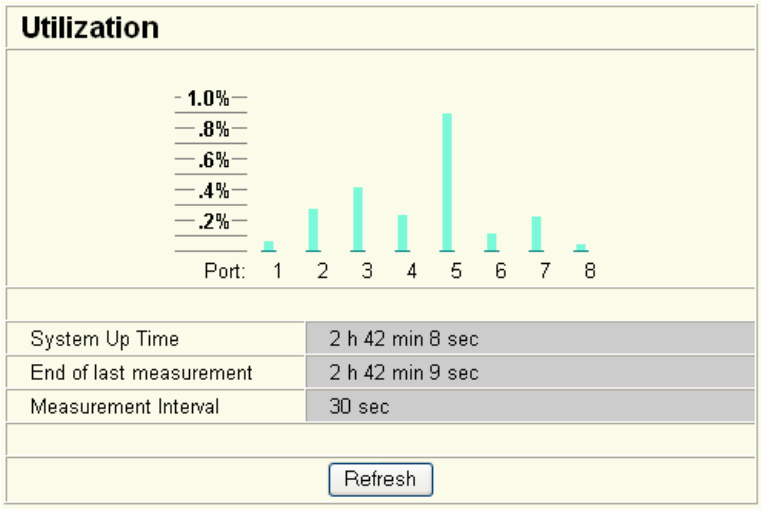


Figure 3-31 Web page „Utilization“

Please observe that the % scale is spread depending on the capacity utilization.

3.2.4.2 Rapid Spanning Tree / Multicast Filtering

For information about (Rapid) Spanning Tree, please refer to Section 4 "Rapid Spanning Tree".

For information about Multicast Filtering, please refer to Section 5 "Multicast Filtering".

3.3 Simple Network Management Protocol (SNMP)

3.3.1 General Function

SNMP is a manufacturer-independent standard for Ethernet management and defines commands for reading and writing error and status message information and formats. SNMP is also a structured model, which comprises agents and their relevant MIB (Management Information Base) and a manager. The manager is a software tool, which is executed on a network management station.

The agents are located inside switches, bus terminals, routers, and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager regularly requests and displays this information. The devices can be configured by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

All configuration modifications, which are to take effect after an LMS restart, must be saved permanently using the "flWorkFWCtrlConfSave" object.

SNMP Interface

All managed Factory Line components have an SNMP agent. This agent manages Management Information Base II (MIB 2) according to RFC1213 MIB, bridge MIB, RSTP MIB, RFC1907 MIB, and private SNMP objects from Phoenix Contact.

Network management stations, such as a PC with the Factory Manager, can read and modify configuration and diagnostic data from network devices via the Simple Network Management Protocol (SNMP). In addition, any SNMP tools or network management tools can be used to access Factory Line products via SNMP. The MIBs supported by the relevant device must be made available to the SNMP management tools.

On the one hand, these are globally valid MIBs, which are specified and described in RFCs (Request for Comments). This includes, for example, MIB2 according to RFC1213, which is supported by all SNMP-compatible network devices. On the other hand, manufacturers can specify their own private SNMP objects, which are then assigned to a private manufacturer area in the large SNMP object tree. Manufacturers are then responsible for their own private (enterprise) areas, i.e., they must ensure that only one object is assigned to an object ID (object name and parameters) and can be published. If an object is no longer needed, it can be labeled as "expired", but it cannot be reused with other parameters under any circumstances.

Phoenix Contact provides notification of ASN1 SNMP objects by publishing their descriptions on the Internet.

Reading SNMP objects is not password-protected. However, a password is required for read access in SNMP, but this is set to "public", which is usual for network devices, and cannot be modified. By default upon delivery, the password for write access is "private" and can be changed by the user.

SNMP, the web interface, Telnet, and the serial terminal all use the same password, which can be changed by the user.

Another benefit for the user is the option of sending traps using the Simple Network Management Protocol.

Management Information Base (MIB)

Database, which contains all the data (objects and variables) required for network management.

Agent

An agent is a software tool, which collects data from the network device on which it is installed, and transmits this data on request. Agents reside in all managed network components and transmit the values of specific settings and parameters to the management station. On a request from a manager or on a specific event, the agent transmits the collected information to the management station.

Traps

Traps are spontaneous SNMP alarm or information messages, which are sent by an SNMP-compatible device when specific events occur. Traps are transmitted with maximum priority to various addresses (if required) and can then be displayed by the management station in plain text. The IP addresses that are to receive these traps (trap targets/receivers) must be set by the user on the relevant device. The following traps are used:

trapColdStart

OID	1.3.6.1.6.3.1.1.5.1
Description	Sent when the switch is started

trapPortUp/Down

OID	1.3.6.1.6.3.1.5.3/4
Description	Sent when a port is switched on or off.

3.3.2 Diagram of SNMP Management

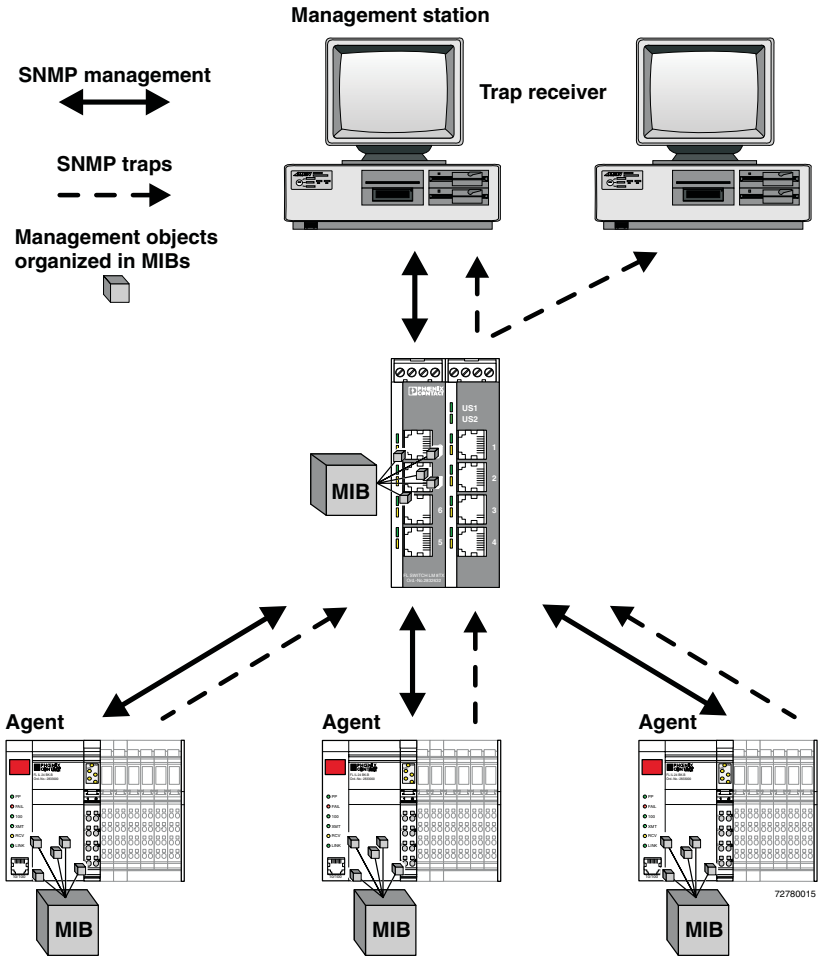


Figure 3-32 Diagram of SNMP

3.3.2.1 Tree Structure of the MIB

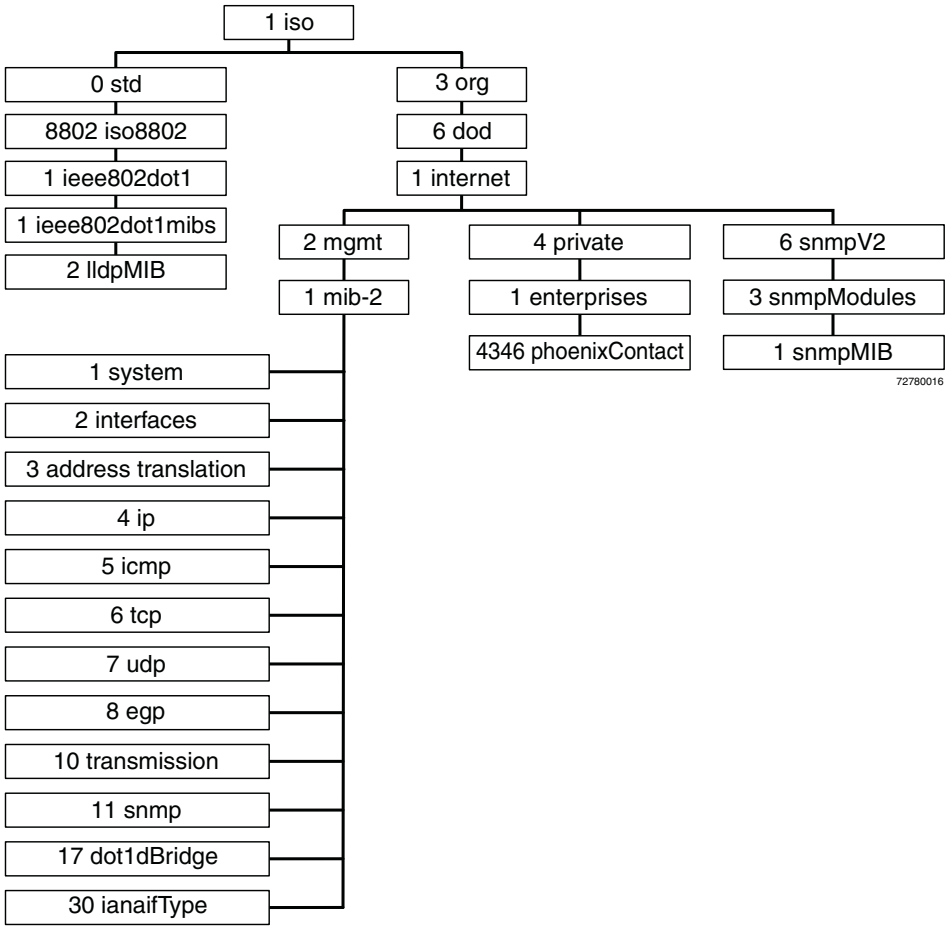


Figure 3-33 Tree structure of the MIB

Not all devices support all object classes. If an unsupported object class is requested, "not supported" is generated. If an attempt is made to modify an unsupported object class, the message "badValue" is generated.

3.3.3 RFC1213-MIB - MIB II

3.3.3.1 System Group (1.3.6.1.2.1.1)

The system group has mandatory characters for all systems. It contains system-specific objects. If an agent does not have a value for a variable, the response is a string with length 0.

(1) system

- (1) sysDescr
- (2) sysObjectID
- (3) sysUpTime
- (4) sysContact
- (5) sysName
- (6) sysLocation
- (7) sysServices
- (8) sysORLastChange
- (9) sysORTable

sysDescr

OID	1.3.6.1.2.1.1.1.0
Syntax	Octet string (size: 0 - 255)
Access	Read
Description	A textual description of the entry. The value should contain the full name and version number of: - Type of system hardware - Operation system software - Network software The description may only consist of ASCII characters that can be printed.

sysObjectID

OID	1.3.6.1.2.1.1.2.0
Syntax	Object identifier
Access	Read
Description	The authorization identification for the manufacturer of the network management subsystem, which is integrated in this device. This value is located in the SMI enterprises subtree (1.3.6.1.4.1) and describes which type of device is being managed. For example: if the manufacturer "Phoenix Contact GmbH" is assigned subtree 1.3.6.1.4.1.4346, it can then assign its bridge the identifier 1.3.6.1.4.1.4346.2.1.

sysUpTime

OID	1.3.6.1.2.1.1.3.0
Syntax	TimeTicks
Access	Read
Description	The time in hundredths of seconds since the last network management unit reset.

sysContact

OID	1.3.6.1.2.1.1.4.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	The textual identification of the contact person for these managed nodes and information on how this person can be contacted.

sysName

OID	1.3.6.1.2.1.1.5.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	A name for this node assigned by the administrator. According to the agreement, this is the fully qualifying name in the domain.

sysLocation

OID	1.3.6.1.2.1.1.6.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	The physical location of this node (e.g., "Hall 1, 3rd floor").

sysServices

OID	1.3.6.1.2.1.1.7.0
Syntax	Integer (0 - 127)
Access	Read
Description	This value indicates a number of services that this device offers. It is the sum of several calculations. For every layer of the OSI reference model, there is a calculation in the form of (2^{L-1}), where L indicates the layer. For example: A node, which primarily executes line routing functions has the value $(2^{3-1}) = 4$. A node, which is a host and provides application services, has the value $(2^{4-1}) + (2^{7-1}) = 72$.

sysORLastChange

OID	1.3.6.1.2.1.1.8
Syntax	TimeTicks
Access	Read
Description	Indicates the value of the sysUpTime during the last system modification.

3.3.3.2 Interface Group (1.3.6.1.2.1.2)

The interface group contains information about device interfaces.

(2) interfaces
-- (1) ifNumber
-- (2) ifTable
-- (1) if Entry
-- (1) ifIndex
-- (2) ifDescr
-- (3) ifType
-- (4) ifMtu
-- (5) ifSpeed
-- (6) ifPhysAddress
-- (7) ifAdminStatus
-- (8) ifOperStatus
-- (9) ifLastChange
-- (10) ifInOctets
-- (11) ifInUcastPkts
-- (12) ifInNUcastPkts
-- (13) ifInDiscards
-- (14) ifInErrors
-- (15) ifInUnknownProtos
-- (16) ifOutOctets
-- (17) ifOutUcastPkts
-- (18) ifOutNUcastPkts
-- (19) ifOutDiscards
-- (20) ifOutErrors
-- (21) ifOutQLen
-- (22) ifSpecific

3.3.4 Bridge MIB (1.3.6.1.2.1.17)

3.3.4.1 dot1dBase (1.3.6.1.2.1.17.1)

The dot1dBase group contains bridge-specific information.

(1) dot1dBaseBridgeAddress
(2) dot1dBaseNumPorts
(3) dot1dBasePortType
(4) dot1dBasePortTable
-- dot1dBasePortEntry
-- (1) dot1dBasePort
-- (2) dot1dBasePortIfIndex
-- (3) dot1dBasePortPortCircuit
-- (4) dot1dBasePortDelayExceededDiscards
-- (5) dot1dBasePortMtuExceededDiscards

3.3.4.2 dot1dStp (1.3.6.1.2.1.17.2)

-- (1) dot1dStpProtocolSpecification
-- (2) dot1dStpPriority
-- (3) dot1dStpTimeSinceTopologyChange
-- (4) dot1dStpTopChanges
-- (5) dot1dStpDesignateRoot
-- (6) dot1dStpRootCost
-- (7) dot1dStpRootPort
-- (8) dot1dStpMaxAge
-- (9) dot1dStpHelloTime
-- (10) dot1dStpHoldTime
-- (11) dot1dStpForwardDelay
-- (12) dot1dStpBridgeMaxAge
-- (13) dot1dStpBridgeHelloTime
-- (14) dot1dStpBridgeForwardDelay
-- (15) dot1dStpPortTable
    -- (1) dot1dStpPortEntry
        -- (1) dot1dStpPort
        -- (2) dot1dStpPortPriority
        -- (3) dot1dStpPortState
        -- (4) dot1dStpPortEnable
        -- (5) dot1dStpPortPathCost
        -- (6) dot1dStpPortDesignatedRoot
        -- (7) dot1dStpPortDesignatedCost
        -- (8) dot1dStpPortDesignatedBridge
        -- (9) dot1dStpPortDesignatedPort
        -- (10) dot1dStpPortForwardTransitions
        -- (11) dot1sStpPortProtocolMigration
        -- (12) dot1dStpPortAdminEdgePort
        -- (13) dot1dStpPortOperEdgePort
        -- (14) dot1dStpPortAdminPointToPoint
        -- (15) dot1dStpPortOperPointToPoint
        -- (16) dot1dStpPortAdminPathCost

3.3.4.3 dot1dSr (1.3.6.1.2.1.17.3)

3.3.4.4 dot1dTp (1.3.6.1.2.1.17.4)

The dot1dTp group contains bridge-specific information.

(1) dot1dTpLearnedEntryDiscards
(2) dot1dTpAgingTime
(3) dot1dTpFdbTable
    -- (1) dot1dTpFdbEntry
        -- (1) dot1dTpFdbAddress
        -- (2) dot1dTpFdbPort
        -- (3) dot1dTpFdbStatus
(4) dot1dTpPortTable
    -- dot1dTpPortEntry
        -- (1) dot1dTpPort

-- (2) dot1dTpPortMaxInfo
-- (3) dot1dTpPortInFrames
-- (4) dot1dTpPortOutFrames
-- (5) dot1dTpPortInDiscards

(5) dot1dTpHCPortTable
-- dot1dTpHCPortEntry
-- (1) dot1dTpHCPortInFrames
-- (2) dot1dTpHCPortOutFrames
-- (3) dot1dTpHCPortInDiscards

(6) dot1dTpPortOverflowTable
-- dot1dTpPortOverflowEntry
-- (1) dot1dTpPortInOverflowFrames
-- (2) dot1dTpPortOutOverflowFrames
-- (3) dot1dTpPortInOverflowDiscards

3.3.4.5 dot1Static (1.3.6.1.2.1.17.5)

-- (1) dot1StaticTable
-- (1) dot1StaticEntry
-- (1) dot1StaticAddress
-- (2) dot1StaticReceivePort
-- (3) dot1StaticAllowedToGoTo

3.3.5 Private MIBs

The private MIBs for the LMS from Phoenix Contact can be found under object ID 1.3.6.1.4.1.4346. The LMS MIB contains the following groups:

– pxcModules (OID = 1.3.6.1.4.1.4346.1)
– pxcGlobal (OID = 1.3.6.1.4.1.4346.2)
– pxcFactoryLine (OID = 1.3.6.1.4.1.4346.11)

All configuration modifications, which are to take effect after an LMS restart, must be saved permanently using the "flWorkFWCtrlConfSave" object.

MIB Tree

The private MIB from Phoenix Contact is integrated in the MIB tree as follows (see red arrow).

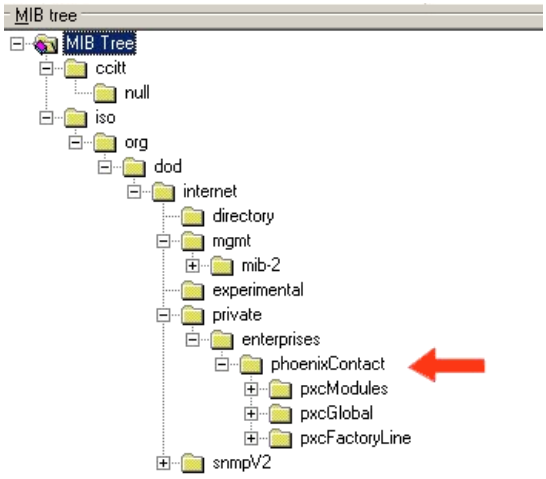


Figure 3-34 MIB tree

3.3.5.1 pxcModules OID = 1.3.6.1.4.1.4346.1

flMSwitchMModule

OID 1.3.6.1.4.1.4346.1.8

The object contains information about the manufacturer (address, phone number, etc.).

3.3.5.2 pxcGlobal OID = 1.3.6.1.4.1.4346.2

pxcBasic

OID 1.3.6.1.4.1.4346.2.1

pxcBasicName

OID 1.3.6.1.4.1.4346.2.1.1

Syntax Display string

Access	Read
Description	Contains the manufacturer's name: Phoenix Contact GmbH & Co. KG.
	pxcBasicDescr
OID	1.3.6.1.4.1.4346.2.1.2
Syntax	Display string
Access	Read
Description	Contains the manufacturer's name and address: Phoenix Contact GmbH & Co. KG P.O. Box 1341 D-32819 Blomberg.
	pxcBasicURL
OID	1.3.6.1.4.1.4346.2.1.3
Syntax	Display string
Access	Read
Description	Contains the manufacturer's web address: http://www.phoenixcontact.com.

3.3.5.3 pxcFactoryLine OID = 1.3.6.1.4.1.4346.11

	flGlobal
OID	1.3.6.1.4.1.4346.11.1
	flBasic
OID	1.3.6.1.4.1.4346.11.1.1
	flBasicName
OID	1.3.6.1.4.1.4346.11.1.1.1
Syntax	Display string
Access	Read
Description	Contains the name of the product group: Factory Line.
	flBasicDescr
OID	1.3.6.1.4.1.4346.11.1.1.2
Syntax	Display string
Access	Read

Description	Contains a brief description of the product group: Ethernet Installation System.
	flBasicURL
OID	1.3.6.1.4.1.4346.11.1.1.3
Syntax	Display string
Access	Read
Description	Contains a specific URL for the product group: www.factoryline.de.
	flBasicCompCapacity
OID	1.3.6.1.4.1.4346.11.1.1.4
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains the number of different components that can be managed with this device.
	flComponents
OID	1.3.6.1.4.1.4346.11.1.2
	flComponentsTable
OID	1.3.6.1.4.1.4346.11.1.2.1
	flComponentsTableEntry

OID	1.3.6.1.4.1.4346.11.1.2.1.1
Syntax	
Access	
Description	Generates a table with descriptions for components in the "Factory Line" product group, which can be managed by this management unit.
flComponentsIndex	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains the product index for the component.
flComponentsName	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.2
Syntax	Display string
Access	Read
Description	Contains the designation of the component.
flComponentsDescr	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.3

Syntax	Display string
Access	Read
Description	Contains a brief description of the component.
flComponentsURL	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.4
Syntax	Display string
Access	Read
Description	Contains the URL of a website with additional information: www.factoryline.de.
flComponentsOrderNumber	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.5
Syntax	Display string
Access	Read
Description	Contains the Order No. of the component.

flWorkDevice

OID 1.3.6.1.4.1.4346.11.11

flWorkBasic

OID 1.3.6.1.4.1.4346.11.11.1

flWorkBasicName

OID	1.3.6.1.4.1.4346.11.11.1.1
Syntax	Display string
Access	Read/write
Description	Contains the device name (corresponds to "sysName" from MIB2).

flWorkBasicDescr

OID	1.3.6.1.4.1.4346.11.11.1.2
Syntax	Display string
Access	Read/write
Description	Contains a brief description (corresponds to "sysDescr" from MIB2).

flWorkBasicURL

OID	1.3.6.1.4.1.4346.11.11.1.3
Syntax	Display string
Access	Read
Description	Contains the URL of the device-specific web page for WBM in the form of the currently set IP address.

flWorkBasicSerialNumber

OID	1.3.6.1.4.1.4346.11.11.1.4
Syntax	Octet string (12)
Access	Read
Description	Contains the serial number of the device.

flWorkBasicHWRevision

OID	1.3.6.1.4.1.4346.11.11.1.5
Syntax	Octet string (4)
Access	Read
Description	Contains the hardware version of the device.

flWorkBasicPowerStat

OID	1.3.6.1.4.1.4346.11.11.1.6
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains status information about the connected supply voltages: - Unknown 1 - Supply voltage 1 OK 3 - Supply voltage 2 OK 4 - Supply voltage 1 and 2 OK 5

flWorkBasicCompMaxCapacity

OID	1.3.6.1.4.1.4346.11.11.1.11
Syntax	Integer 32
Access	Read
Description	Contains the maximum number of interfaces that can be connected.

flWorkBasicCompCapacity

OID	1.3.6.1.4.1.4346.11.11.1.12
Syntax	Integer 32
Access	Read
Description	Contains the number of interfaces actually connected.

flWorkComponentsGroup

OID 1.3.6.1.4.1.4346.11.11.2

flWorkNet

OID 1.3.6.1.4.1.4346.11.11.4

flWorkNetIfParameter

OID 1.3.6.1.4.1.4346.11.11.4.1

flWorkNetIfParamPhyAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.1
Syntax	MAC address
Access	Read
Description	Contains the MAC address of the switch.

flWorkNetIfParamIPAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.2
Syntax	IP address
Access	Read/write
Description	Contains the current IP address of the LMS. Modifications only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamSubnetmask

OID	1.3.6.1.4.1.4346.11.11.4.1.3
Syntax	IP address
Access	Read/write
Description	Contains the current subnet mask of the LMS. Modifications only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamGWIpAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.4
Syntax	IP address
Access	Read/write
Description	Contains the IP address of the current default gateway/router of the LMS. Modifications only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamStatus

OID	1.3.6.1.4.1.4346.11.11.4.1.5
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Indicates whether the IP parameters have been modified but not saved: - No change 1 - Address setting modified, but not yet activated 2

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetIfParamSave

OID	1.3.6.1.4.1.4346.11.11.4.1.6
Syntax	Integer
Access	Read/write
Description	Provides the option of saving modified IP parameters or undoing the modifications: - Undo modification 1 - Activate modification 2

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetIfParamAssignment

OID	1.3.6.1.4.1.4346.11.11.4.1.7
Syntax	Integer
Access	Read/write
Description	Provides the option of modifying the assignment mechanism for IP parameters. Takes effect after an LMS restart: - Static IP address 1 - Assignment via BootP 2

Modifications to the assignment mechanism also affect the management functions via the web interface, via V.24 (RS-232), and Telnet.

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetPort

OID	1.3.6.1.4.1.4346.11.11.4.2

flWorkNetPortCapacity

OID	1.3.6.1.4.1.4346.11.11.4.2.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains the number of available ports depending on the configuration of the LMS.

flWorkNetPortTable

OID 1.3.6.1.4.1.4346.11.11.4.2.2

flWorkNetPortEntry

OID	1.3.6.1.4.1.4346.11.11.4.2.2.1
Description	Generates a table with a detailed description of the port configuration.
flWorkNetPortIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Specifies the port number of the selected port.
flWorkNetPortLinkState	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.2
Syntax	Integer
Access	Read
Description	Indicates the port status: Connected 1 Not connected 2 farEndFault
flWorkNetPortSpeed	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.3
Syntax	Gauge32
Access	Read
Description	Contains the data transmission rate of the selected port in bps.
flWorkNetPortDuplexMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.4
Syntax	INTEGER
Access	Read
Description	Contains the duplex mode of the selected port: Full duplex 1 Half duplex 2
flWorkNetPortNegotiation	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.5
Syntax	INTEGER
Access	Read

Description	Contains the duplex mode of the selected port: Automatic 1 Manual 2
flWorkNetPortName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.6
Syntax	Octet string (0 - 16)
Access	Read/write
Description	Contains the "name" of the port, e.g., "Robot 1".
flWorkNetPortEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.7
Syntax	Integer
Access	Read/write
Description	Here you can disable the port: Port disabled 1 Port enabled 2
flWorkNetPortLinkMonitoring	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.8
Syntax	Integer
Access	Read/write
Description	This object can be used to enable link monitoring (message via display and alarm contact) for the relevant port: Link monitoring enabled 2 Link monitoring disabled 1
flWorkNetPortModus	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.9
Syntax	Integer32 (0 - 1024)
Access	Read/write
Description	This object can be used to set the transmission mode for the relevant port: Auto negotiation 1 10 Mbps half duplex 2 10 Mbps full duplex 3 100 Mbps half duplex 4 100 Mbps full duplex 5 Glass fiber FX ports only support operation at 100 Mbps full duplex (5). The auto crossing function is only active when auto negotiation is enabled. If the transmission speed or transmission mode is set to a fixed value, the auto crossing function is disabled.
flWorkNetPortIfIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.11
Syntax	Integer32 (0 - 1024)

Access	Read
Description	Contains the index of the port according to IEEE 802.3ad.
flWorkNetPortType	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.13
Syntax	Octet string
Access	Read
Description	Specifies the medium of this port.
flWorkNetPortModuleName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.14
Syntax	Octet string
Access	Read
Description	Specifies the "name" of the module.
flWorkNetPortInterfaceName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.15
Syntax	Octet string
Access	Read
Description	Specifies the "name" of the interface.
flWorkNetPortPofTransmittingPower	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.17
Syntax	Integer
Access	Read
Description	For polymer fiber (POF) paths < 20 m the transmission power must be reduced.
	Transmission power unknown 1 Transmission power low 2 Transmission capacity standard 3
flWorkNetPortStpMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.18
Syntax	Integer
Access	Read
Description	Specifies the port mode during redundancy operation:
	Spanning Tree 1 Rapid Spanning Tree 2

flWorkFirmware

OID 1.3.6.1.4.1.4346.11.11.11

flWorkFWInfo

OID 1.3.6.1.4.1.4346.11.11.11.1

flWorkFWInfoVersion

OID	1.3.6.1.4.1.4346.11.11.11.1.1
Syntax	Octet string (4)
Access	Read
Description	Contains the firmware version as a string. Example for Version "3.97": 0x33, 0x2e, 0x39, 0x37.

flWorkFWInfoState

OID	1.3.6.1.4.1.4346.11.11.11.1.2
Syntax	Octet string (6)
Access	Read
Description	Contains the firmware release as a string. Example for "beta": 0x62, 0x65, 0x64, 0x61.

flWorkFWInfoDate

OID	1.3.6.1.4.1.4346.11.11.11.1.3
Syntax	Octet string (6)
Access	Read
Description	Contains the creation date of the firmware version as a string. Example for "21.05.2001": 0x32, 0x31, 0x30, 0x35, 0x30, 0x31.

flWorkFWInfoTime

OID	1.3.6.1.4.1.4346.11.11.11.1.4
Syntax	Octet string (6)
Access	Read
Description	Contains the creation time of the firmware version as a string. Example for "14:10:20": 0x31, 0x34, 0x31, 0x30, 0x32, 0x30.

flWorkFWInfoCopyright

OID	1.3.6.1.4.1.4346.11.11.11.1.5
Syntax	Display string (6)
Access	Read
Description	Contains the owner of the firmware copyright. Copyright by Phoenix Contact GmbH & Co., 2003.

flWorkFWInfoBootVersion

OID	1.3.6.1.4.1.4346.11.11.11.1.6
Syntax	Octet string (4)
Access	Read
Description	Contains the version of the Boot loader as a string. Example for Version "2.65": 0x32, 0x2e, 0x36, 0x35.

flWorkFWInfoBootState

OID	1.3.6.1.4.1.4346.11.11.11.1.7
Syntax	Octet string (6)
Access	Read
Description	Contains the Boot loader release as a string. Example for "beta": 0x62, 0x65, 0x64, 0x61.

flWorkFWInfoBootDate

OID	1.3.6.1.4.1.4346.11.11.11.1.8
Syntax	Octet string (6)
Access	Read
Description	Contains the creation date of the Boot loader version as a string. Example for "09.03.01": 0x30, 0x39, 0x30, 0x33, 0x30, 0x31.

flWorkFWInfoBootTime

OID	1.3.6.1.4.1.4346.11.11.11.1.9
Syntax	Octet string (6)
Access	Read
Description	Contains the creation time of the Boot loader version as a string. Example for "14:10:20": 0x31, 0x34, 0x31, 0x30, 0x32, 0x30.

flWorkFWCtrl

OID 1.3.6.1.4.1.4346.11.11.11.2

flWorkFWCtrlBasic

OID 1.3.6.1.4.1.4346.11.11.11.2.1

flWorkFWCtrlReset

OID	1.3.6.1.4.1.4346.11.11.11.2.1.1
Syntax	Integer
Access	Read/write
Description	With write access, a reset can be executed with "2". With read access, the value is always "1". When a reset is triggered, "rb" is indicated in the display.

flWorkFWCtrlHttp

OID	1.3.6.1.4.1.4346.11.11.11.2.1.6
Syntax	Integer
Access	Read/write
Description	This object can be used to disable the web server for the switch. The modification only takes effect after a restart: Web server enabled: 2 Web server disabled: 1

flWorkFWCtrlSNMP

OID	1.3.6.1.4.1.4346.11.11.11.2.1.9
Syntax	Integer
Access	Read/write
Description	Here you can activate/deactivate the SNMP agent. The modifications take effect following a restart. SNMP agent deactivated 1 SNMP agent activated 2

flWorkFWCtrlTrapDest

1.3.6.1.4.1.4346.11.11.11.2.2

flWorkFWCtrlTrapDestTable

1.3.6.1.4.1.4346.11.11.11.2.2.1

flWorkFWCtrlTrapDestEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1
Syntax	
Access	
Description	Generates a table with the IP addresses of the trap managers.
flWorkFWCtrlTrapDestIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains the index of the target component, which should receive the traps.
flWorkFWCtrlTrapDestIPAddr	

OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.2
Syntax	IP address
Access	Read/write
Description	Contains the IP address of the target component, which should receive the traps.

flWorkFWCtrlTrapDestCapacityMax

OID	1.3.6.1.4.1.4346.11.11.11.2.2.2
Syntax	Integer32
Access	Read
Description	Contains the maximum permissible number of trap receivers.

flWorkFWCtrlTrapDestEnable

OID	1.3.6.1.4.1.4346.11.11.11.2.2.3
Syntax	Integer
Access	Read/write
Description	This object can be used to disable the "send SNMP traps" function: Sending permitted 2 Sending not permitted 1

flWorkFWCtrlPasswd

OID 1.3.6.1.4.1.4346.11.11.11.2.3

flWorkFWCtrlPasswdSet

OID	1.3.6.1.4.1.4346.11.11.11.2.3.1
Syntax	Octet string (2 - 24)
Access	Read/write

For security reasons, the response is always "*****" for read access.

Description

A new password can be entered here with a maximum of 12 characters. Example:
- Your new password should be "*factory3*".
- The password must be entered a second time for confirmation.
- Your entry "*factory3factory3*".
- Your password for write access is now: "*factory3*".

flWorkFWCtrlPasswdSuccess

OID	1.3.6.1.4.1.4346.11.11.11.2.3.2
Syntax	Integer
Access	Read
Description	A message is displayed, which informs you whether the last change of password was successful: - Not changed 1 - Failed 2 - Successful 3

flWorkFWCtrlLoginExpire

OID	1.3.6.1.4.1.4346.11.11.11.2.3.3
Syntax	Integer32 (30 - 3600)
Access	Read/write
Description	Here, the number of seconds between two password entries is specified. After the time has elapsed, the password must be re-entered, if required. Default 300 Range 30 - 3600

flWorkFWCtrlUpdate

OID 1.3.6.1.4.1.4346.11.11.11.2.4

flWorkFWCtrlTftpIpAddr

OID	1.3.6.1.4.1.4346.11.11.11.2.4.2
Syntax	IP address
Access	Read/write
Description	This object can be used to set the IP address of the TFTP server.

flWorkFWCtrlTftpFile

OID	1.3.6.1.4.1.4346.11.11.11.2.4.3
Syntax	Octet string (0 - 64)
Access	Read/write
Description	This object can be used to set the name of the firmware file for TFTP download.

flWorkFWCtrlUpdateStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.4.4
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the firmware update:

Update successful	1
Update not successful	2
No update completed	3
Unknown	4

flWorkFWCtrlUpdateExecute

OID	1.3.6.1.4.1.4346.11.11.11.2.4.5
Syntax	Integer
Access	Read/write
Description	This object can be used to trigger the firmware update.

No firmware update	1
Execute firmware update	2

After a firmware update, a reset is required to activate the new firmware.

flWorkFWCtrlRunningUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4.6
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the firmware update:

Firmware update not started	1
Executing firmware update	2
Firmware update successful	3
Connection error	4
Incorrect file name	5
Error	6

flWorkFWCtrlAutoUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4.7
Syntax	Integer
Access	Read/write
Description	This object can be used to trigger the firmware update with subsequent restart:

No firmware update	1
Execute firmware update	2

flWorkFWCtrlConf

OID 1.3.6.1.4.1.4346.11.11.11.2.5

flWorkFWCtrlConfStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.1
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the active device configuration:

Configuration OK	1
Configuration faulty	2
Configuration saved	3
Saving configuration	4

flWorkFWCtrlConfSave

OID	1.3.6.1.4.1.4346.11.11.11.2.5.2
Syntax	Integer
Access	Read/write
Description	This object can be used to save the device configuration:

Do not save configuration	1
Save configuration	2

flWorkFWCtrlDefaultUponDelivery

OID	1.3.6.1.4.1.4346.11.11.11.2.5.3
Syntax	Integer
Access	Read/write
Description	This object can be used to set the device to the default settings (basic settings - see 2.1.1 on page 2-1). It also triggers a restart:

Do not reset to default settings	1
Reset to default settings	2

flWorkFWCtrlSerial

OID 1.3.6.1.4.1.4346.11.11.11.2.6

flWorkFWCtrlSerialBaud

OID	1.3.6.1.4.1.4346.11.11.11.2.6.1
Syntax	Integer
Access	Read
Description	This object can be used to request the set data transmission rate of the serial interface:

2400 baud	1
9600 baud	2
19200 baud	3
38400 baud	4
57600 Baud	5
115200 Baud	6

flWorkFWCtrlSerialDataBits

OID	1.3.6.1.4.1.4346.11.11.11.2.6.2
Syntax	Integer
Access	Read
Description	Contains the number of data bits in the serial interface: 8 bit 1

flWorkFWCtrlSerialStopBits

OID	1.3.6.1.4.1.4346.11.11.11.2.6.3
Syntax	Integer
Access	Read
Description	Contains the number of stop bits in the serial interface: 1 bit 1 2 bits 2

flWorkFWCtrlSerialParity

OID	1.3.6.1.4.1.4346.11.11.11.2.6.4
Syntax	Integer
Access	Read
Description	Contains the parity mode for the serial interface: None 1 Odd 2 Even 3

flWorkFWCtrlSerialFlowControl

OID	1.3.6.1.4.1.4346.11.11.11.2.6.5
Syntax	Integer
Access	Read
Description	Contains the selected flow control for the serial interface: None 1 Hardware 2

flSwitch

OID 1.3.6.1.4.1.4346.11.11.15

flSwitchCtrl

OID 1.3.6.1.4.1.4346.11.11.15.1

flSwitchCtrlSpanTree

OID	1.3.6.1.4.1.4346.11.11.15.1.1
Syntax	Integer
Access	Read/write
Description	Activates/deactivates STP for the switch.

RSTP deactivated	1
RSTP activated	2

To enable RSTP activation, the "flSwitchCtrlRedundancy" object must be set to RSTP.

flSwitchCtrlRedundancy

OID	1.3.6.1.4.1.4346.11.11.15.1.2
Syntax	Integer
Access	Read/write
Description	Displays the selected redundancy mechanisms for the switch. If "No redundancy" is selected, all redundancy mechanisms and the corresponding web pages are disabled.

No redundancy	1
RSTP activated	2

For RSTP configuration, the Bridge_MIB is used, see page 3-32.

flSwitchCtrlMacTableErase

OID	1.3.6.1.4.1.4346.11.11.15.1.11
Syntax	Integer
Access	Read/write
Description	This object is used to control the Unicast clear function. Upon being set to a value of “2” the Unicast table will immediately clear all of its entries. The switch will then resume learning addresses normally and rebuilding the Unicast table. The value of the OID will revert back to “1”.

Default	1
Clear Unicast table	2

flSwitchIgmpTableErase

OID	1.3.6.1.4.1.4346.11.11.15.3.3
Syntax	Integer
Access	Read/write
Description	This object is used to control the Multicast clear function. Upon being set to a value of “2” the Unicast table will immediately clear all of its entries. The switch will then resume learning addresses normally and rebuilding the Multicast table. The value of the OID will revert back to “1”.

Default	1
Clear Multicast table	2

3.4 Management via Local V.24 (RS-232) Communication Interface

3.4.1 General Function

A local communication connection can be established to an external management station via the V.24 (RS-232) interface in Mini-DIN format. Use the "PRG CAB MINI DIN" programming cable (Order No. 2730611). The communication connection is established using a corresponding emulation between the switch and a PC (e.g., HyperTerminal under Windows) and enables access to the user interface.

The reference potentials of the V.24 (RS-232) interface and the supply voltage are not electrically isolated.

3.4.1.1 Interface Configuration

Make the following settings on your Windows PC.

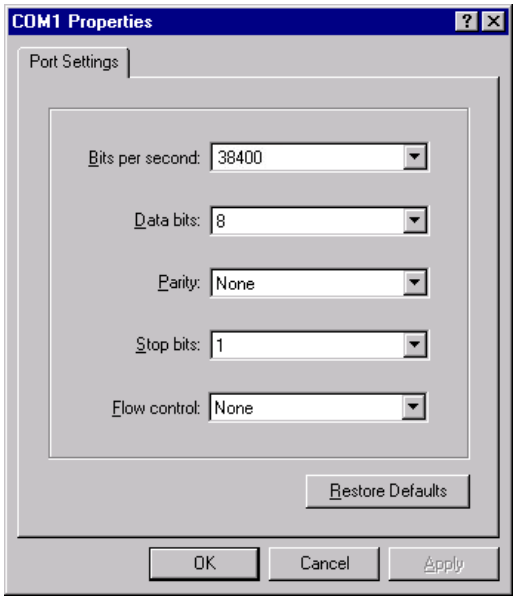


Figure 3-35 Configuring the HyperTerminal

3.4.1.2 Calling the User Interface

Connect the PC and the switch using a suitable V.24 (RS-232) cable (PRG CAB MINI DIN, Order No. 2730611). Once you have made the connection, select the Ctrl + L key combination on the PC. The switch then requests the screen contents.

3.4.2 User Interface Functions

3.4.2.1 Functions During the Boot Process After a Restart

If you open the user interface in the first five seconds directly after an LMS restart, you have the option of triggering a firmware update. Since the actual switch firmware is not yet started at this stage, even in the event of an error, e.g., if the firmware on the device is faulty, this firmware can still be updated (see "Starting With Faulty Software" on page 3-56).

3.4.2.2 Functions During Operation

The following functions are available in the user interface:

– Setting IP parameters
– Selecting the addressing mechanism
– Resetting to Default Settings
– Activating/deactivating the web server, Rapid Spanning Tree, SNMP interface, and the Telnet function.

The activation/deactivation of the web server only takes effect after a "SAVE" and subsequent restart.

All settings are transferred using "APPLY", but are **not** saved permanently. Use the "SAVE" function to save the active configuration settings permanently.

3.4.2.3 Structure of the User Interface Screens

Login Screen

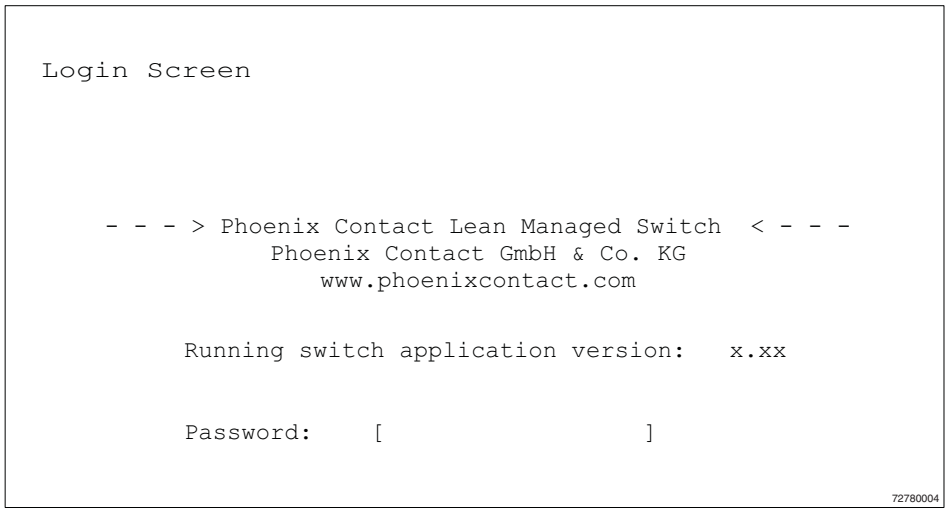

Login Screen
- - - > Phoenix Contact Lean Managed Switch < - - -
Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com
Running switch application version: x.xx
Password: [ ]
72780004

Figure 3-36 User interface login screen

The login screen indicates the version of the firmware used. A password must be entered to make other settings. By default upon delivery, the password is "private". It is case-sensitive. We strongly recommend that you change the password (via SNMP or WBM).

Basic Switch Configuration

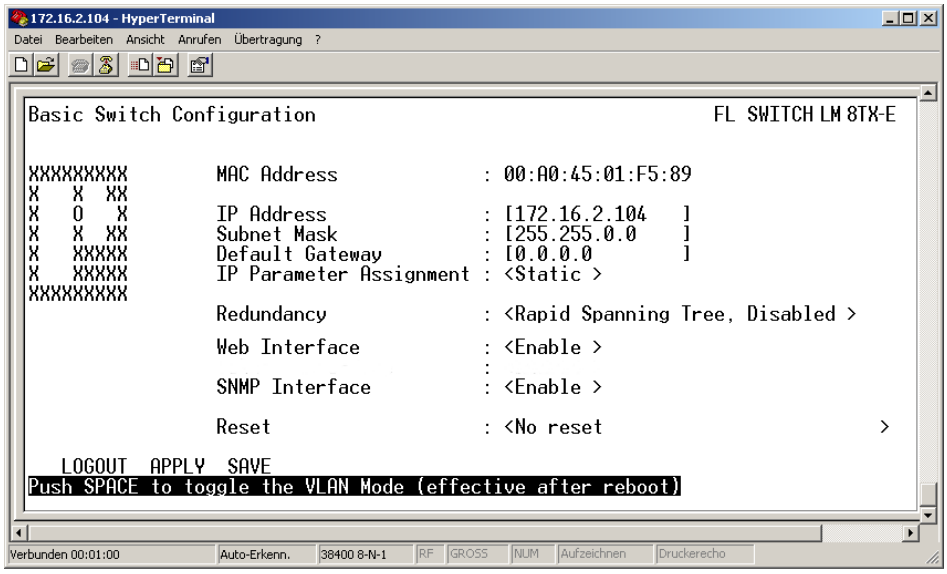


Figure 3-37 IP configuration in the user interface

As well as displaying the set MAC address, this screen can be used to view or modify the IP parameters.

In order to set the IP parameters, the "Static" option must be selected for "IP Parameter Assignment".

This user interface screen can be used to determine the addressing mechanism or to trigger a device restart.

All settings are transferred using "APPLY", but are **not** saved permanently. Use the "SAVE" function to save the active configuration settings permanently.

Resetting to Default Settings

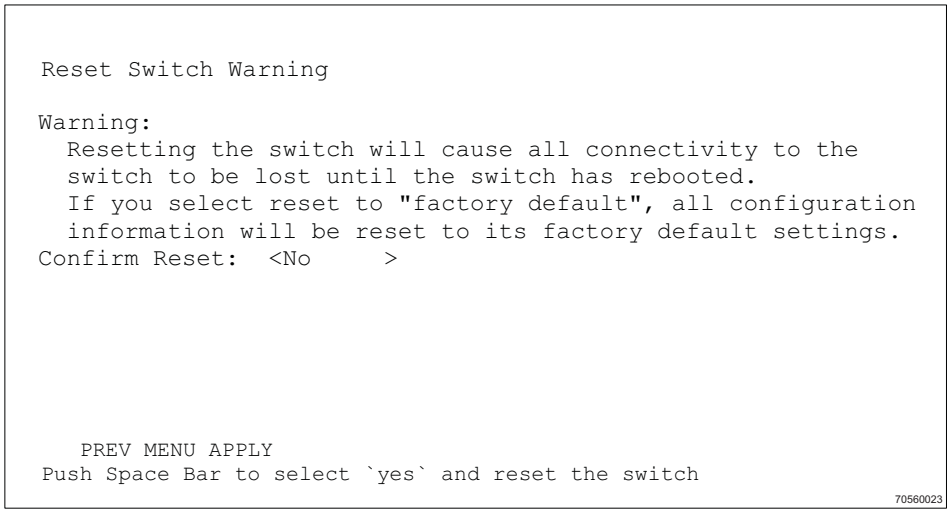

Reset Switch Warning
Warning:
Resetting the switch will cause all connectivity to the switch to be lost until the switch has rebooted.
If you select reset to "factory default", all configuration information will be reset to its factory default settings.
Confirm Reset: <No >
PREV MENU APPLY
Push Space Bar to select `yes` and reset the switch
70560023

Figure 3-38 Resetting to default settings

This screen can be used to reset the switch to the settings default upon delivery or to restart it. This screen can be opened by first setting the "Reset Switch" option or the "Reset Switch to factory defaults" option in the "Basic Switch Configuration" screen, and then selecting "Apply" or "Save". This undoes any changes to the configuration, and resets all IP parameters to the settings default upon delivery (see Section 2.1.1 on page 2-1).

Resetting to the default settings also resets the password to "private". For security reasons, we recommend you enter a new, unique password.

3.4.3 Starting With Faulty Software

If the software installed on the LMS (firmware) is faulty, you can restore or update the firmware using an update.

Procedure:

– Connect the switch to your PC via the serial V.24 (RS-232) interface. Make sure that your HyperTerminal is configured correctly (see configuration on page 3-52).

```
- - - > Phoenix Contact Lean Managed Switch < - - -

Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com
BIOS version: X.XX


Press any key to stop booting ...
1

ENTER ´a´  TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´  TO CONTINUE BOOTING

PxC LMS systemprompt
```

70560024

Figure 3-39 Screen displayed on HyperTerminal when booting

If the device firmware is faulty, the following message appears:

```
     - - - > Phoenix Contact Lean Managed Switch < - - -
                Phoenix Contact GmbH & Co. KG
                   www.phoenixcontact.com


Press any key to stop booting ...
 0
booting continues ...

SOFTWARE IMAGE CORRUPTED

YOU HAVE TO UPDATE THE SOFTWARE USING XMODEM PROTOCOL:

ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING

PxC LMS systemprompt>
```

72780005

Figure 3-40 Selection menu for faulty firmware

Press "a" to download the new software. The following message appears:

```
     - - - > Phoenix Contact Lean Managed Switch < - - -
                 Phoenix Contact GmbH & Co. KG
                    www.phoenixcontact.com



ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING

PxC LMS systemprompt> a

Downloading firmware image with XMODEM over serial port ...

XMODEM Receive: Waiting for Sender ...

-_
```

72780006

Figure 3-41 XMODEM ready

The switch is now ready for the new firmware. In HyperTerminal, select "Send File" from the "Transmission" menu.

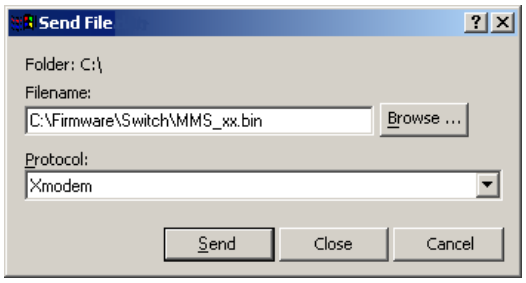


Figure 3-42 Xmodem - Send File option

Make sure that the protocol is set to "Xmodem", otherwise the transmission will fail.

Clicking "Send" starts the file transfer. The following screen shows the progress of the file transmission.

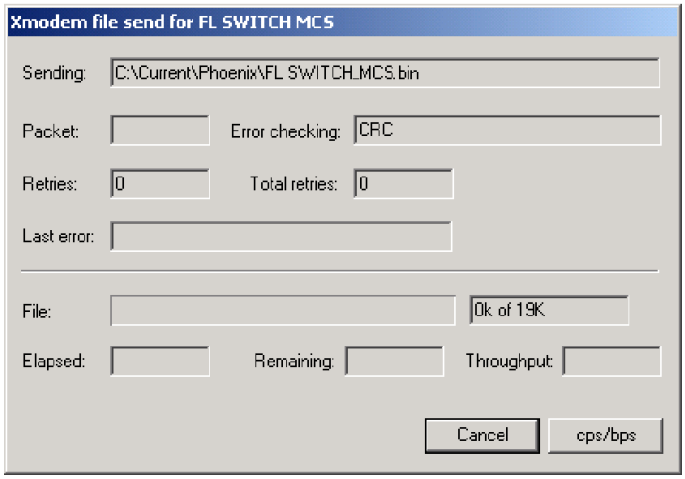


Figure 3-43 File transmission with Xmodem

File transmission may take a few minutes. Do not perform any other actions while the box is open.

Once the box has closed, a message appears in HyperTerminal. Enter "c" to continue with the boot process, or trigger a reset using the reset button.

4 Rapid Spanning Tree

4.1 General Function

4.1.1 General Function

Loops

The Rapid/Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.802.1w/IEEE 802.1d) that enables the use of Ethernet networks with redundant data paths. Ethernet networks with redundant data paths form a meshed topology with impermissible loops. Due to these loops, data packets can circulate endlessly within the network and can also be duplicated. As a consequence, the network is usually overloaded due to circulating data packets and thus communication is interrupted. The meshed structure is thus replaced by a logical, deterministic path with a tree structure without loops using the Spanning Tree algorithm. In the event of data path failure, some of the previously disconnected connections are reconnected to ensure uninterrupted network operation.

IEEE 802.1w

The Rapid Reconfiguration Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.1w) that enables the use of Ethernet networks with redundant data paths and prevents the long timer-controlled switch-over times of STP. Usually, the formal term "Rapid Reconfiguration Spanning Tree" is not used, rather just "Rapid Spanning Tree Protocol (RSTP)".

Example:

In the following network topology (six) redundant paths have been created to ensure access to all network devices in the event of a data path failure. These redundant paths are impermissible loops. The RSTP protocol automatically converts this topology into a tree by disconnecting selected ports. In this context, one of the switches is assigned the role of the root of the tree. From this root, all other switches can be accessed by via a single data path.

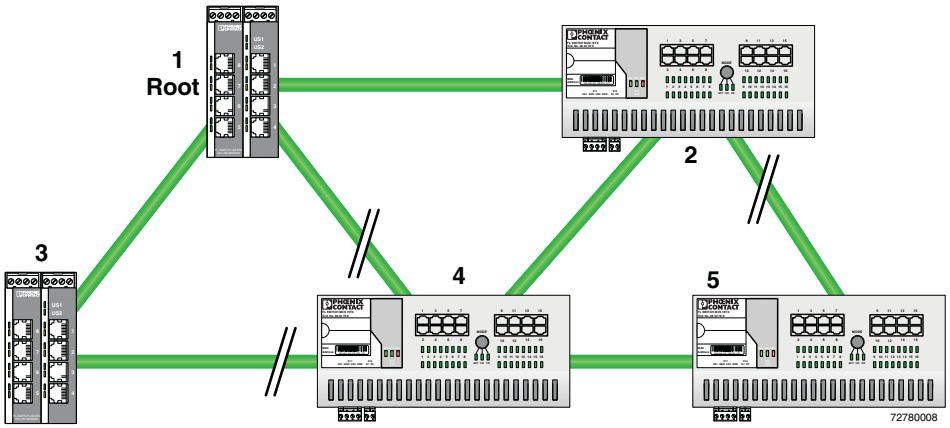


Figure 4-1 Possible tree structure with Spanning Tree

4.2 RSTP Startup

Startup consists of two parts that must be executed in the specified order:

1 Enable RSTP on all switches that are to be operated as active RSTP components in the network.

2 Connect the switches to form a meshed topology.

Only create the meshed topology after activating RSTP.

4.2.1 Enabling RSTP on All Switches Involved

RSTP can be activated via web-based management, via the SNMP interface, via the serial interface or via Telnet.

While learning the network topology, the switch temporarily does not participate in network communication.

4.2.1.1 Enabling With Web-Based Management

Activate web-based management for the switches, e.g., using the Factory Manager, switch to the "General Configuration" menu, then the "User Interfaces" page. Activate the "(Rapid) Spanning Tree" function under "Redundancy" and confirm by entering your password.

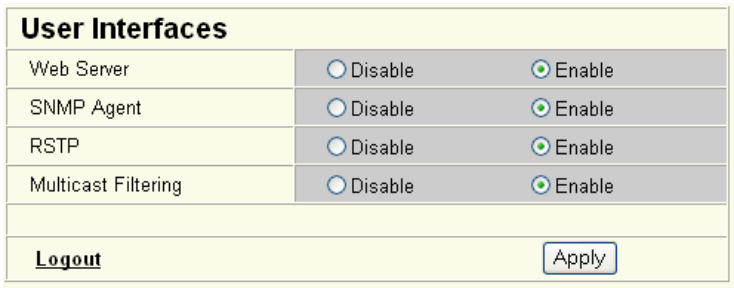
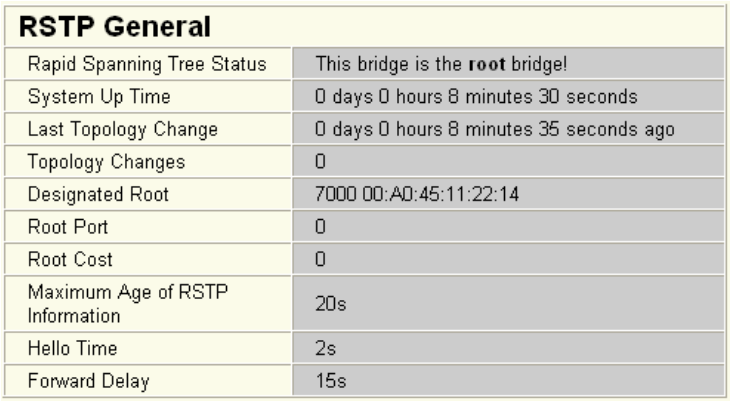


Figure 4-2 "User Interfaces" menu

The previously created configuration is lost if "No redundancy" is selected in the WBM menu following RSTP configuration.

Now switch to the "RSTP General" menu. Here, you will find various information about the Spanning Tree configuration.



RSTP General	
Rapid Spanning Tree Status	This bridge is the **root** bridge!
System Up Time	0 days 0 hours 8 minutes 30 seconds
Last Topology Change	0 days 0 hours 8 minutes 35 seconds ago
Topology Changes	0
Designated Root	7000 00:A0:45:11:22:14
Root Port	0
Root Cost	0
Maximum Age of RSTP Information	20s
Hello Time	2s
Forward Delay	15s

Figure 4-3 "RSTP General" web page

The web page displays the parameters with which the switch is currently operating.

Port Roles

The **root port** of a switch connects this switch to the root switch - either directly or via another switch (designated switch).

The **designated port** is the port at a designated switch that is connected to the root port of the next switch.

No additional switches/bridges are connected to **edge ports**. Termination devices are connected to edge ports.

An **alternate port** is a path to the root, which, however, did not become a root port. I.e., this port is not part of the active topology.

RSTP Configuration

It is sufficient to set the Rapid Spanning Tree status to "Enable" in order to start RSTP using default settings. Priority values can be specified for the switch. The root and alternate ports can be specified via these priority values.

Only multiples of 4096 are permitted. The desired value can simply be entered in the "Priority" field. The value will be rounded automatically to the next multiple of 4096. Once you have confirmed the modification by entering your password, the initialization mechanism is started.

Redundant connections can now be created.

The "Maximum Age of STP Information", "Hello Time", and "Forward Delay" fields have the same meaning as for STP. These values are used when this switch becomes a root. The values currently used can be found under RSTP General.

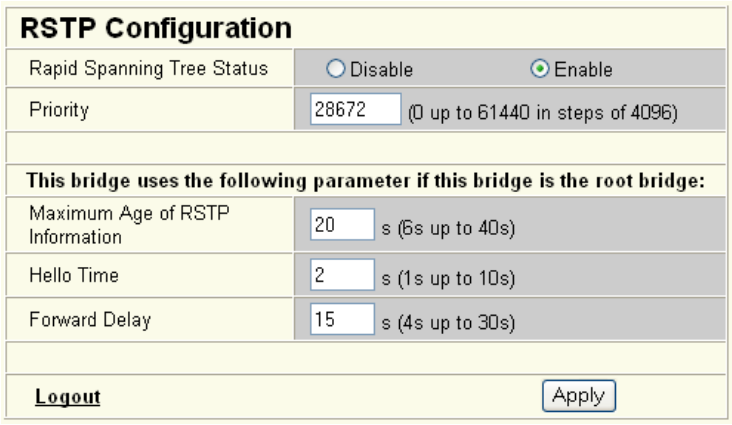


Figure 4-4 "RSTP Configuration" web page

Maximum Age of STP Information
STP information (BPDU) is sent by the root switch at an age of "0" and at hello time intervals. If a BPDU was received, every other switch sends its own configuration message via the ports for which the switch itself is the designated switch. The age of the information (BPDU) is increased by one second every time the information passes a switch.

Hello Time
Specifies the time interval within which the root bridge regularly reports to the other bridges via BPDU.

Forward Delay
The forward delay value indicates how long the switch is to wait in order for the port state in STP mode to change from "Discarding" to "Listening" and from "Listening" to "Learning" (2 x forward delay).

RSTP Port Table

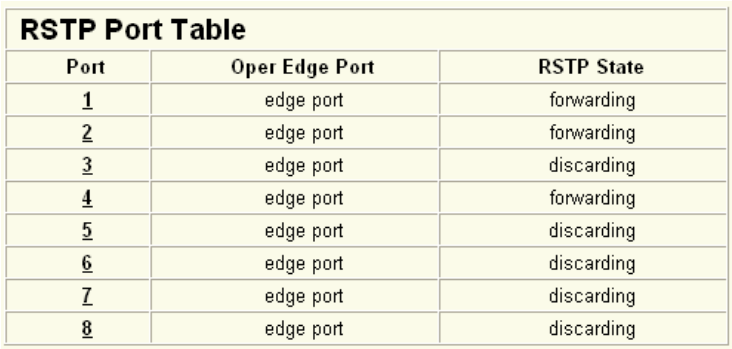


Figure 4-5 "RSTP Port Table" web page

Oper Edge Port
All ports that do not receive any RSTP BPDUs become edge ports, i.e., ports that switch to the "Forwarding" state immediately after restart.

RSTP State
Indicates the current RSTP state of the relevant port.

Possible states:

– "Forwarding"
  The port is integrated in the active topology and forwards data.
– "Discarding"
  The port does not take part in data transmission.
– "Learning"
  The port does not take part in data transmission of the active topology, however, MAC addresses are learned.

4.2.1.2 RSTP Port Configuration

Modifications of properties can result in complete reconfiguration of (Rapid) Spanning Tree.

This page displays the valid RSTP configuration settings for the selected port.

If termination devices or subnets are connected without RSTP or STP via a port, it is recommended to set the "Admin Edge Port" to "Edge Port". In this way, a link modification at this port does not result in a topology modification.

4.2.1.3 Switch/Port ID

The validity of switches and ports is determined according to priority vectors.

Bridge Identifier

A switch ID consists of 8 bytes as an unsigned integer value. When comparing two switch IDs, the one with the lowest numeric value is of higher, i.e., "better" priority.

The first two bytes contain the priority.
The last 6 bytes contain the MAC address and thus ensure the uniqueness of the switch ID in the event of identical priority values.

The switch with the lowest numerical switch ID becomes the root. It is recommended that the root port and alternate port are specified using the priority.

Port Identifier

The port ID consists of 4 bits for the port priority and 12 bits for the port number. The port ID is interpreted as an unsigned integer value. When comparing two port IDs, the one with the lowest numeric value is of higher, i.e., "better" priority.

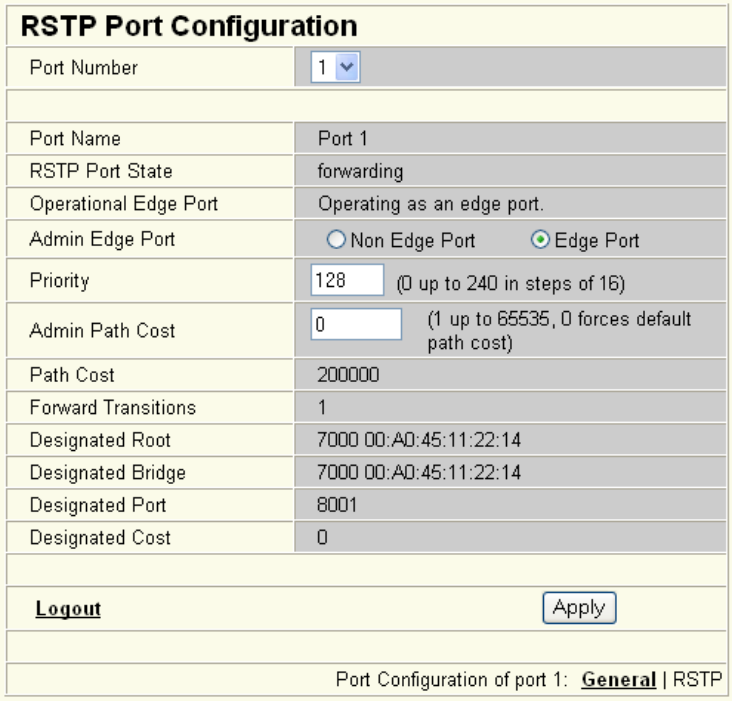


Figure 4-6 "RSTP Port Configuration" web page

Port Number
Indicates the number of the port currently selected.

Port Name
Indicates the name of the port.

STP Port State
Indicates the status in which this port takes part in STP.

Operational Edge Port
Indicates whether this port is operated as an edge port.

Admin Edge Port
Here you can specify whether this port is to be operated as an edge port (default setting), if possible.

Priority
Indicates the priority set for this port. Due to backwards compatibility with STP, priority values can be set that are not configurable in RSTP.

Admin Path Cost
Indicates the path costs set for this port. A path cost equal to "0" activates the cost calculation according to the transmission speed (10 Mbps = 100; 100 Mbps = 19).

Path Cost
Indicates the path costs used for this port.

Forward Transitions
Indicates how often the port switches from the "Discarding" state to the "Forwarding" state.

Additional parameters provide information about network paths in a stable topology that are used by the BPDU telegrams.

Designated Root
Root bridge for this Spanning Tree.

Designated Bridge
The switch from which the port receives the best BPDUs. The value is based on the priority value in hex and the MAC address.

Designated Port
Port via which the BPDUs are sent from the designated bridge. The value is based on the port priority (2 digits) and the port number.

Designated Cost
It indicates the path costs of this segment to the root switch.

Common features/differences with regard to STP

As with STP, a device is also selected as the root for RSTP and every port is assigned a role according to its participation within the topology.

Port States

The number of port states is also reduced in RSTP. Only the "Forwarding", "Discarding", and "Learning" states are still available if the network is operated in mixed operation of STP and RSTP.

Frame duplication

Due to the fast switch-over times of RSTP, frames may be duplicated and the order of frames may be changed.

4.2.1.4 Enabling via Serial Interface

Establish a connection to the switch as described in "Management via Local V.24 (RS-232) Communication Interface" on page 3-52. Set "Spanning Tree, Enabled" on the following page in the "Redundancy" field and select "Save".

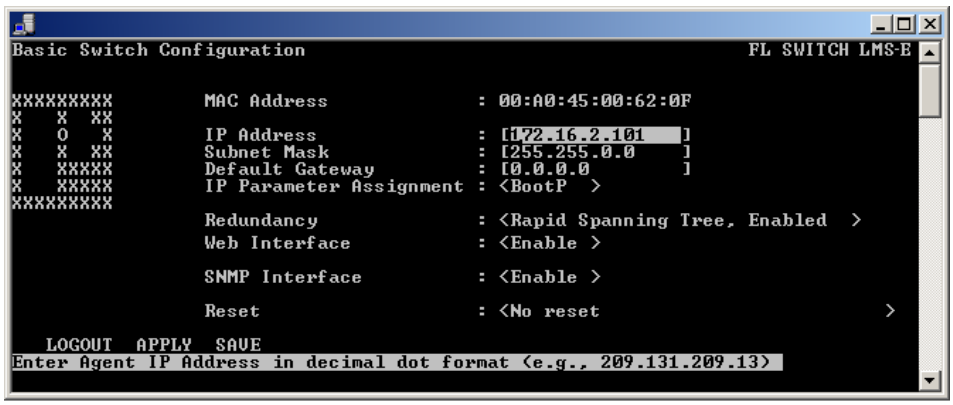


Figure 4-7 Activating Spanning Tree

4.2.1.5 Connecting the Switches to Form a Meshed Topology

Having activated (Rapid) Spanning Tree for all switches, you can create a meshed topology with redundant data paths. Any data connections can now be created without taking loops into consideration. Loops can even be added on purpose in order to create redundant connections.

A data path between Spanning Tree switches can be:

– A direct connection.
– A connection via one or more additional switches that do not support Spanning Tree.

If Spanning Tree is not supported by all of the switches used, the reconfiguration time for Spanning Tree is extended by the aging time of switches without Spanning Tree support.

– A connection via one or more additional hubs that do not support Spanning Tree.

Furthermore, a data path can also consist of a connection of a Spanning Tree switch to:

– A termination device.
– A network segment in which **no** loops may occur, which consists of several infrastructure components (hubs or switches) without Spanning Tree support.

For the first three scenarios, the following rules must be observed:

– **Rule 1: Spanning Tree transparency for all infrastructure components**
  All infrastructure components used in your network that do not actively support Spanning Tree must be transparent for Spanning Tree messages (BPDUs) and must forward all BPDUs to all ports without modifying them. When Spanning Tree is disabled, the switch is transparent for BPDUs.
– **Rule 2: At least one active Spanning Tree component per loop**
  An active Spanning Tree component supports the Spanning Tree Protocol, sends/receives and evaluates BPDUs, and sets its ports to the relevant STP states. Each loop in a network must have at least one active Spanning Tree component to disintegrate the loop.

Example:

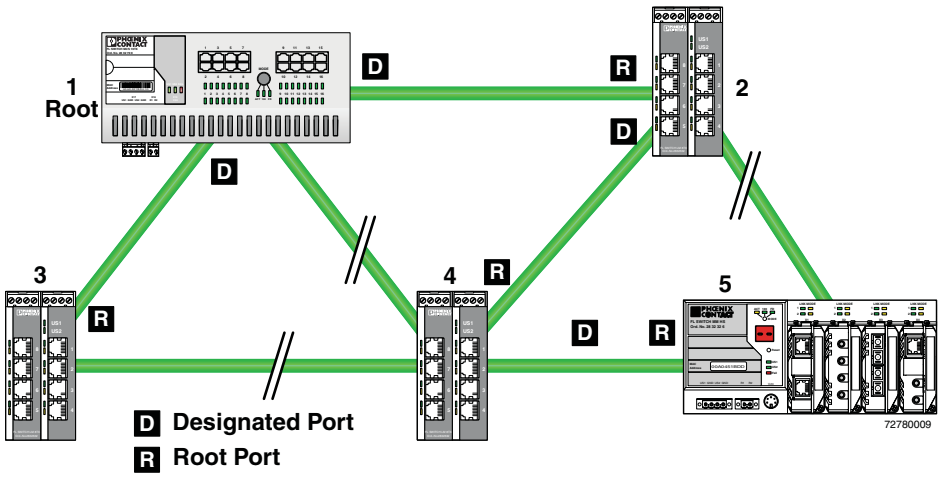


Figure 4-8 Example topology

The example topology shown above contains six loops. Each of these loops contains active STP components, e.g., device 4 and device 2. In this way, all loops are broken by STP.

– **Rule 3: No more than ten active Spanning Tree components in the topology when using Spanning Tree default settings**
  The ability to disintegrate any topology to form a tree without loops requires a complex protocol that works with several variable timers. These variable timers are dimensioned using IEEE standard default values so that a topology with a maximum of ten active Spanning Tree components always results in a stable network.

4.2.1.6 Example Topologies

4.2.1.7 Redundant Coupling of Network Segments

In this example, two network segments are connected via redundant data paths. Two STP components have ports in the "Blocking" state (highlighted in gray). This is sufficient to operate the network.

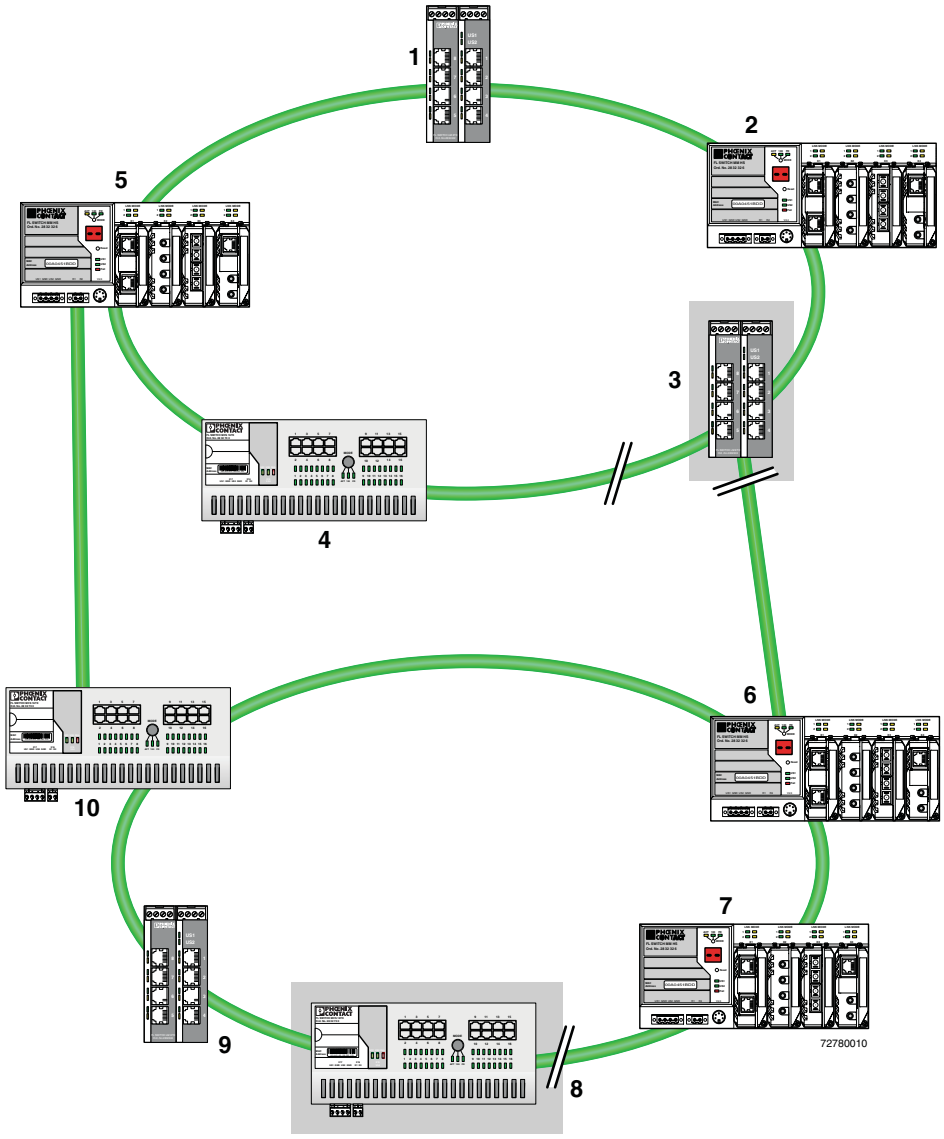


Figure 4-9 Redundant coupling of network segments

4.2.1.8 Flowchart for Specifying the Root Path

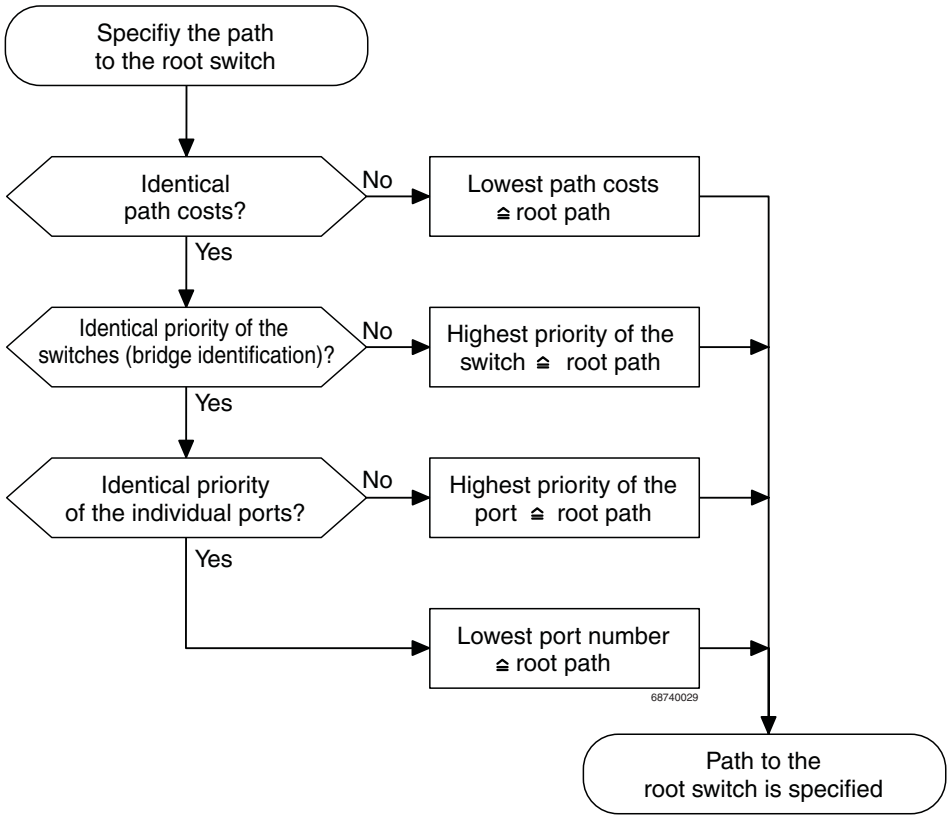


Figure 4-10 Flowchart for specifying the root path

4.2.1.9 Extended Configuration

It may be useful to actively specify the topology that is formed due to the Spanning Tree Protocol and to not leave it to the random MAC addresses of the switches involved. Non-blocking/blocking data paths can thus be influenced and a load distribution specified. It may also be useful to explicitly disable the Spanning Tree Protocol at ports that do not participate in Spanning Tree so as to benefit from the fast forwarding function.
The Spanning Tree Protocol must also be disabled at individual ports if two different network segments - both using Spanning Tree - are to be coupled via these ports without the two tree structures melting into a large Spanning Tree.

Specifying the Root Switch

The root switch is assigned via the assignment of an appropriate priority for the Spanning Tree segment. Set the highest priority (lowest value) in the "Priority" field on the "STP Bridge Configuration" page in WBM for the switch selected as the root switch. Make sure that all the other network switches have a lower priority (higher value). Here, the set path costs are not evaluated.

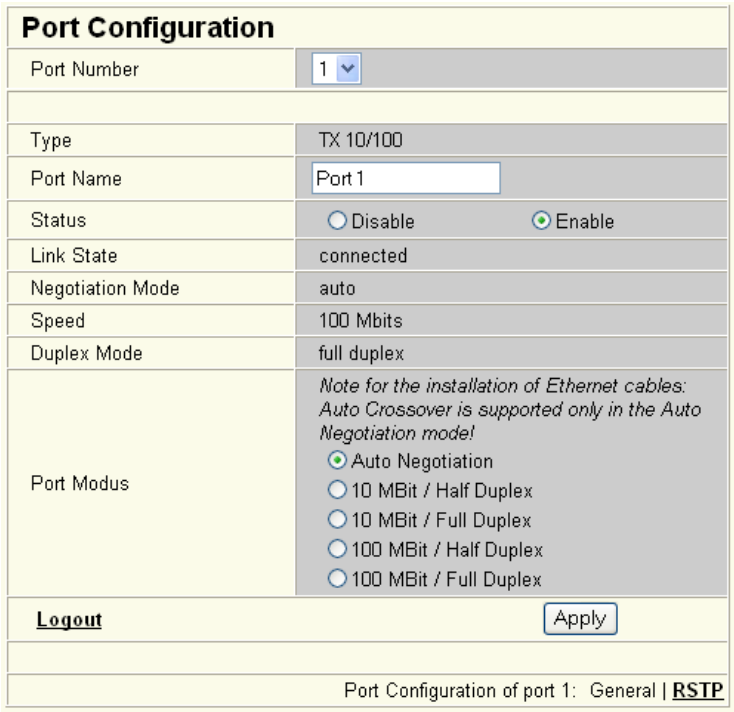


Figure 4-11 Specifying the root switch priority

Specifying the Root Port and Designated Port

The root port and designated port are always the ports with the lowest path costs. If the costs are the same, the priority is the decisive criterion. If the priorities are also the same, the port number is the decisive criterion. Specify an appropriate combination of costs and priority on the "STP Port Configuration" page in WBM for the port specified as the root port or designated port. Make sure that all the other network switches either have higher costs or a lower priority (higher value).

4.2.1.10 Disabling the Spanning Tree Protocol/Using the Fast Forwarding Function

One of the following requirements must be met so that the Spanning Tree Protocol can be disabled for a port:

– A termination device is connected to the port.
– Additional infrastructure components are connected to the port. The corresponding network segment does not contain any loops.
– Additional infrastructure components are connected to the port, forming a Spanning Tree of their own. No additional redundant connections to this network segment are permitted.

4.2.1.11 Modifying the Protocol Timer

Modifying the protocol timer may result in unstable networks.

It may be necessary to modify the protocol timer if, e.g., there are more than ten active Spanning Tree components in a single network. You can also attempt to reduce the reconfiguration times by modifying the timer. However, care should be taken in order to prevent unstable networks.
Please note that the protocol times are specified by the root switch and that they are distributed to all devices via BPDU. It is therefore only necessary to modify the values in the root switch. If the root switch fails, the timer values of another active STP switch (i.e., the new root switch) will be valid for the entire network segment. Please remember this during component configuration.

Specifying the Timer Values

– Maximum number of active Spanning Tree components along the path beginning at the root switch (please refer to the following two example illustrations):
  = (MaxAge/2) - Hello Time + 1
– 2 x Forward Delay - 1 s ≥ MaxAge
– MaxAge ≥ 2 × Hello Time + 1 s

The value ((MaxAge/2) - Hello Time) for a ring topology corresponds to the maximum number of components with active Spanning Tree.

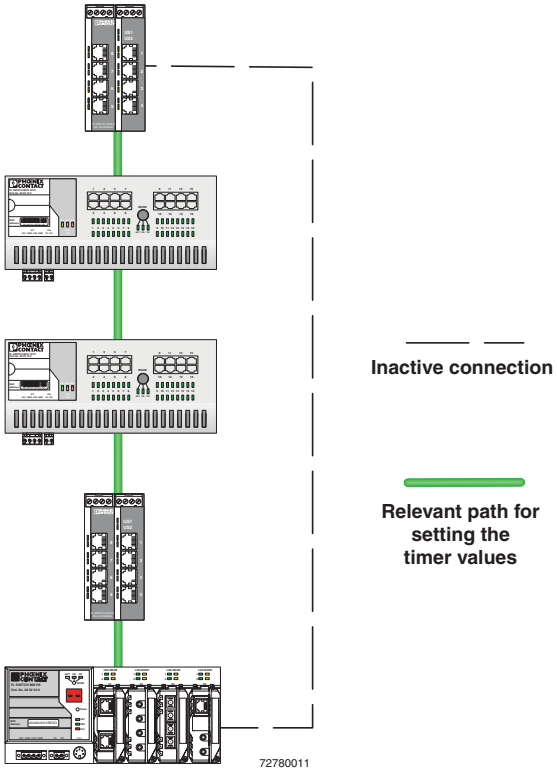


Figure 4-12 Example 1 for the "relevant path"

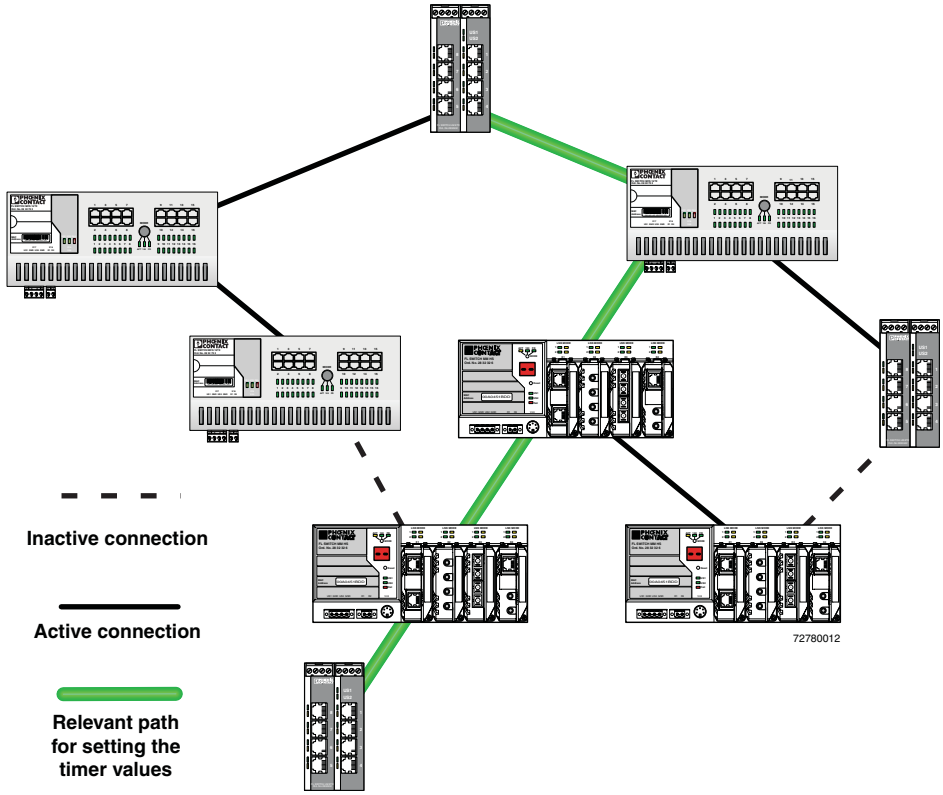


Figure 4-13 Example 2 for the "relevant path"

4.2.1.12 Reconfiguration Times

The reconfiguration time for a Spanning Tree depends on the timer values for MaxAge and Forward Delay.

The minimum reconfiguration time is:
2 × Forward Delay

The maximum reconfiguration time is:
2 × Forward Delay + MaxAge

For the values recommended by the IEEE standard, the value for ten active STP switches along a path beginning with the root switch is between 30 s and 50 s.

Switch-Over Time Response to Be Expected for Spanning Tree

Overview of the switch-over time response to be expected for the maximum number of switches within a Spanning Tree segment.

MaxAge	Hello Time	Forward Delay	Maximum Number of Active STP Switches	Switch-Over Time
10 s	1 s	≥ 6 s	5	22 s
20 s	1 s	≥ 11 s	10	42 s
30 s	1 s	≥ 16 s	15	62 s
40 s	1 s	≥ 21 s	20	82 s
20 s	***2 s***	***15 s***	***9***	***50 s***

Bold/italic **= Default**

4.2.2 Configuration Notes for Rapid Spanning Tree

In contrast to the Spanning Tree method, the Rapid Spanning Tree method supports event-controlled actions that are no longer triggered based on a timer.

If one cable fails (link down), the Rapid Spanning Tree method can respond more quickly to this failure and thus the switch-over time can be kept low.

A link down or link up must be detected at the switch so that the RSTP switches can detect a line failure and a restored line more quickly. Please take into consideration, in particular, paths where media converters are used. If required, media converters offer setting options to transmit the link status of the fiber optic side to the twisted pair side.

If a link down is not detected at the switch, due to the cable interrupt between the media converters, and if no link down is forced at the switch, timer-based detection is activated, which may result in longer switch-over times.

– For short switch-over times, structure your network in such a way that a maximum of seven switches are located in a cascade up to the root switch. The switch-over times can range from 2 to 8 s.
– Use priority assignment to specify a central switch as the root.
– It is also recommended to assign a switch as the back-up root.
– For short switch-over times, all switches should support the Rapid Spanning Tree Protocol.

5 Multicast Filtering

5.1 Basics

Multicast

Multicast applications - other than Unicast applications using point-to-point communication - do not transmit their data using a MAC address of the target, but they use a multicast group address that is target-independent. Always using wireless communication, a station transmits **one** data packet that is received by one or more receiving stations.

Advantages:

1 In case one data packet of a transmitter is to be transmitted to 8 receivers, the same packet must not be sent 8 times to the addresses of all 8 devices. Instead it only needs to be sent once to the address of the multicast group that includes 8 devices.

2 When using multicast communication and filtering, the required bandwidth for data transmission is reduced because every packet can only be transmitted once.

5.2 Dynamic Multicast Groups

5.2.1 Internet Group Management Protocol - IGMP

IGMP on Layer 3

The Internet Group Management Protocol describes a procedure for distributing information via mulitcast applications between routers and termination devices on the IP level (layer 3).

When starting a multicast application, a network device transmits a so-called IGMP membership report and thus publishes its membership of a specified multicast group. A router collects these membership reports and thus maintains the multicast groups of its sub networks.

Query

At regular intervals, the router transmits IGMP queries. This causes the devices with multicast-receiver applications to transmit a membership report again.

The router enters the IP multicast group address from the report message in its routing table. This means that frames with this IP multicast group address in the target address field are only transferred according to the routing table. Devices that are no longer members of a multicast group log out with a leave message (IGMP Version 2 or later) and no longer send any report messages.
The router also removes the routing table entry if it does not receive a report message within a specific time (aging time). If several routers with active IGMP query function are connected in the network, they determine amongst themselves which router carries out the query function. This depends on the IP address, as the router with the lowest IP address continues to operate as the querier and all the other routers no longer send any query messages. If these routers do not receive a new query telegram within a specific period of time, they themselves become queriers again. If there are no routers in the network, a suitably equipped switch can be used for the query function.

IGMP Snooping

A switch, which connects a multicast receiver with a router, can read and evaluate IGMP information using the IGMP snooping method. IGMP snooping translates IP multicast group addresses into MAC multicast addresses, so that the IGMP function can also be

detected by layer-2 switches. The switch enters the MAC addresses of the multicast receivers, which were obtained from the IP addresses by IGMP snooping, into its own multicast table. Thus the switch filters multicast packets of known multicast groups and only forwards packets to those ports to which corresponding multicast receivers are connected.

IGMP snooping can only be used on layer 2 if all termination devices send IGMP messages. The IP stack of multicast termination devices with applications linked to a multicast address automatically sends the relevant membership reports.

IGMP snooping operates independently of the Internet group management protocol (IGMP).

5.2.1.1 Extended Multicast Filtering

When IGMP Snooping is enabled, if the switch receives multicast data for which no IGMP reports have been received and for which no multicast group currently exists, the switch creates the group automatically. This multicast data is then forwarded to the querier, i.e. the querier port is added by default to the group. If the switch itself is the active querier, then these multicasts are blocked on all ports. Any subsequent IGMP reports for this group received on other ports are handled normally, that is, the port is added as a member to the multicast group.

5.2.2 "General Multicast Configuration" Website

This website provides global settings for multicast support. Here, IGMP snooping can be enabled and an aging time can be specified for IGMP snooping information.

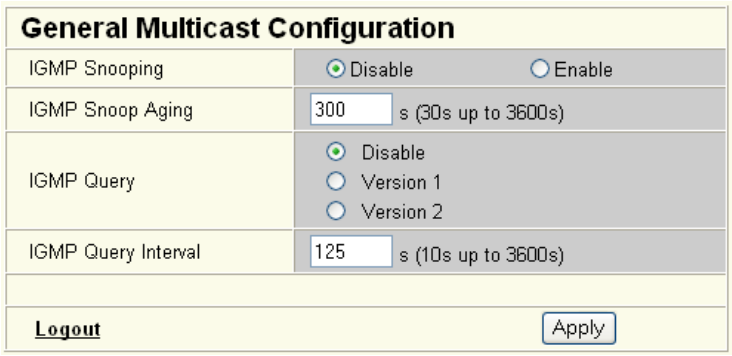


Figure 5-1 "General Multicast Configuration" Website

The switch supports 50 multicast groups at the same time.

IGMP Snooping
In IGMP snooping, the switch passively listens in on the IGMP messages that are sent over the network and dynamically creates the appropriate groups. These groups are not stored and will be lost with every power-down or when switching off the snooping function.

IGMP Query
An LMS with activated query function actively transmits queries at intervals and evaluates the received reports. The LMS only sends IGMP query reports if IGMP snooping is enabled.

5.2.2.1 Multicast Registration with GMRP

GMRP is the GARP Multicast Registration Protocol and it allows the distribution of Multicast Group Destination Addresses to layer two devices that don't support IGMP Snooping. After a multicast participant has registered with the switch (e.g through an IGMP report), the switch sends a GMRP broadcast packet to all GARP participating switches with the Multicast Group Destination Address and whether the switch is joining or leaving. This allows the other switches to create their own multicast groups and add the receiving port to the group. By default GMRP is enabled when IGMP Snooping is enabled. The receiving switches do not need to support IGMP Snooping to receive and understand the GMRP packets they receive.

6 Technical Data

General Data	
Function	Lean Managed Ethernet/Fast Ethernet Switch; conforms to standard IEEE 802.3
Switch principle	Store-and-Forward
Address table	For 1023 MAC addresses
SNMP	Version 1 and 2
Supported MIBs	SNMPv2 MIB, RSTP MIB, and private SNMP objects from Phoenix Contact
Housing dimensions (width x height x depth)	45 mm x 99 mm x 112 mm
Permissible operating temperature	-40°C to +70°C
Permissible storage temperature	-40°C to +85°C
Degree of protection	IP20, DIN 40050, IEC 60529
Protection class	Class 3 VDE 0106; IEC 60536
Maximum humidity (operation)	30% to 95%, no condensation
Maximum humidity (storage/transport)	30% to 95%, no condensation
Air pressure (operation)	86 kPa to 108 kPa, 1500 m above sea level
Air pressure (storage)	66 kPa to 108 kPa, 3500 m above sea level
Preferred mounting position	Perpendicular to a standard DIN rail
Connection to protective earth ground	Snapped onto a grounded DIN rail/via COMBICON (optional)
Weight	140 g, typical

Supply Voltage	
Connection	Via COMBICON; conductor cross section = 2.5 mm^2, maximum
Nominal value	24 V DC
Permissible ripple	3.6 V_{PP} within the permissible voltage range
Permissible voltage range	18.5 V DC to 30.5 V DC
Current consumption at U_S at nominal value	170 mA, typical; 250 mA, maximum
Test voltage	500 V DC for one minute
Protection against polarity reversal	Present
Power consumption	4 W, typical; 6 W, maximum

Interfaces	
Ethernet interface in RJ45 format	
Number	8 or 4
Connection format	8-pos. RJ45 female connector on the switch
Connection medium	Twisted pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 Ohm
Transmission speed	10/100 Mbps
Ethernet interface (SC)	
Number	0 or 2
Connection format	SC duplex female connector on the switch
Wavelength	1300 nm
Laser protection	Class 1 according to DIN EN 60825-1:2001-11
Minimum transmission length, including 3 dB system reserve, when using **multi-**mode	6,4 km glass fiber with F-G 50/125 0,7 dB/km F1200 2,8 km glass fiber with F-G 50/125 1,6 dB/km F800 11 km glass fiber with F-G 62,5/125 0,7 dB/km F100 3,0 km glass fiber with F-G 62,5/125 2,6 dB/km F1000
Maximum transmission power **multi-**mode	-14 dBm
Minimum transmission power **multi-**mode	-20 dBm with 62,5/125 µm, -23,5 with 50/125 µm
Minimum receiver sensitivity **multi-**mode	-31 dBm
Maximum overrange **multi-**mode	-14 dBm

Interfaces (Continued)

Minimum transmission length, including 3 dB system reserve, when using **single**-mode	36 km glass fiber with F-G 9/125 0,36 dB/km 32 km glass fiber with F-G 9/125 0,4 dB/km 26 km glass fiber with F-G 9/125 0,5 dB/km
Maximum transmission power **single-**mode	-8 dBm
Minimum transmission power **single-**mode	-15 dBm
Minimum recierver sensitivity **single-**mode	-31 dBm
Maximum overrange **single-**mode	-7 dBm
Transmission speed	100 Mbps
V.24 (RS-232) communication interface	
Number	1
Connection format	Mini-DIN female connector on the switch
Floating alarm contact	
Voltage	24 V DC
Current carriyng capacity	100 mA, maximum

Mechanical Tests

Shock test according to IEC 60068-2-27	Operation: 25g, 11 ms period, half-sine shock pulse Storage/transport: 50g, 11 ms period, half-sine shock pulse
Vibration resistance according to IEC 60068-2-6	Operation/storage/transport: 5g, 150 Hz, criterion 3
Free fall according to IEC 60068-2-32	1 m

Conformance With EMC Directives

Developed according to IEC 61000-6.2	
Noise emission according to EN55022: 1998 + A1: 2000 + A2: 2003 (interference voltage)	Class A (industrial applications)
Noise emission according to EN55011: 1998 + A1: 1999 + A2: 2002 (electromagnetic interference)	Class A (industrial applications)
Noise immunity according to EN61000-4-2 (IEC1000-4-2) (ESD)	Requirements according to DIN EN 61000-6-2
Contact discharge:	Test intensity 2, criterion B
Air discharge:	Test intensity 3, criterion B
Indirect discharge:	Test intensity 2, criterion B
Noise immunity according to EN61000-4-3 (IEC1000-4-3) (electromagnetic fields)	Requirements according to DIN EN 61000-6-2 Test intensity 3, criterion A
Noise immunity according to EN61000-4-4 (IEC1000-4-4) (burst)	Requirements according to DIN EN 61000-6-2
Data lines:	Test intensity 2, criterion B
Power supply:	Test intensity 3, criterion B
Noise immunity according to EN61000-4-5 (IEC1000-4-5) (surge)	Requirements according to DIN EN 61000-6-2
Data lines:	Test intensity 2, criterion B
Power supply:	Test intensity 1, criterion B
Noise immunity according to EN61000-4-6 (IEC1000-4-6) (conducted)	Requirements according to DIN EN 61000-6-2 Test intensity 3, criterion A

Differences Between This Version and Previous Versions

Version 00: First version
Version 01: LM-E switches and functions of the actual firmware version added

Ordering Data

Products

Description	Type	Order No.	Pcs./Pkt.
Lean managed switch with eight RJ45 ports	FL SWITCH LM 8TX FL SWITCH LM 8TX-E	2832632 2891466	1
Lean managed switch with four RJ45 ports and two multi-mode SC ports	FL SWITCH LM 4TX/2FX FL SWITCH LM 4TX/2FX-E	2832658 2891660	1
Lean managed switch with four RJ45 ports and two single-mode SC ports	FL SWITCH LM 4TX/2FX SM FL SWITCH LM 4TX/2FX SM-E	2891916 2891864	1

Accessories

Description	Type	Order No.	Pcs./Pkt.
Security set for four RJ45 ports	FL SEC PAC 4TX	2832865	4
Gray RJ45 connector set for linear cable	FL PLUG RJ45 GR/2	2744856	2
Green RJ45 connector set for crossed cable	FL PLUG RJ45 GN/2	2744571	2
Universal end clamp	E/NS 35 N	0800886	50
Assembly tool for RJ45 connector	FL CRIMPTOOL	2744869	1
Startup/diagnostic software - Factory Manager	FL SWT	2831044	1
Network monitoring with HMI/SCADA systems	FL SNMP OPC SERVER	2832166	1
Patch box 8 x RJ45 CAT5e, pre-assembled, can be retrofitted	FL PBX 8TX	2832496	1
Patch cable, CAT 5, pre-assembled, 0.3 m long	FL CAT5 PATCH 0,3	2832250	10
Patch cable, CAT 5, pre-assembled, 0.5 m long	FL CAT5 PATCH 0,5	2832263	10
Patch cable, CAT 5, pre-assembled, 1.0 m long	FL CAT5 PATCH 1,0	2832276	10
Patch cable, CAT 5, pre-assembled, 1.5 m long	FL CAT5 PATCH 1,5	2832221	10
Patch cable, CAT 5, pre-assembled, 2.0 m long	FL CAT5 PATCH 2,0	2832289	10
Patch cable, CAT 5, pre-assembled, 3.0 m long	FL CAT5 PATCH 3,0	2832292	10
Patch cable, CAT 5, pre-assembled, 5.0 m long	FL CAT5 PATCH 5,0	2832580	10
Patch cable, CAT 5, pre-assembled, 7.5 m long	FL CAT5 PATCH 7,5	2832616	10
Patch cable, CAT 5, pre-assembled, 10.0 m long	FL CAT5 PATCH 10	2832629	10

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
Germany

+49 - 52 35 - 30 0

+49 - 52 35 - 34 12 00

www.phoenixcontact.com

Worldwide Locations:
www.phoenixcontact.com/salesnetwork

HOTLINE:

Should problems occur that cannot be resolved with the help of this documentation, please contact our hotline:

+49 - 52 35 - 34 18 88